PCT/JP99/02510
EJ

17.06.99

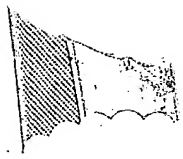
日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

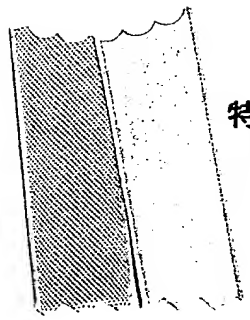
出願年月日
Date of Application: １９９８年１０月２９日

出願番号
Application Number: 平成１０年特許願第３０９２２３号

出願人
Applicant (s): 三菱マテリアル株式会社



１９９９年 ４月 ９日



特許庁長官
Commissioner,
Patent Office 伊佐山建志

出証番号 出証特平１１－３０２１０９３

【書類名】　特許願

【整理番号】　J75130A1

【提出日】　平成10年10月29日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 11/00

【発明の名称】　チームデータリスト管理装置及びチームデータリスト保管装置及びチームデータリスト処理システム、並びに、それらの記録媒体

【請求項の数】　8

【発明者】

【住所又は居所】　埼玉県大宮市北袋町１丁目２９７番地　三菱マテリアル株式会社　総合研究所内

【氏名】　大久保　達真

【発明者】

【住所又は居所】　埼玉県大宮市北袋町１丁目２９７番地　三菱マテリアル株式会社　総合研究所内

【氏名】　中根　一成

【特許出願人】

【識別番号】　000006264

【氏名又は名称】　三菱マテリアル株式会社

【代理人】

【識別番号】　100064908

【弁理士】

【氏名又は名称】　志賀　正武

【選任した代理人】

【識別番号】　100108578

【弁理士】

【氏名又は名称】　高橋　詔男

【選任した代理人】

【識別番号】　100089037

【弁理士】

【氏名又は名称】　渡邊　隆

【選任した代理人】

【識別番号】　100101465

【弁理士】

【氏名又は名称】　青山　正和

【選任した代理人】

【識別番号】　100094400

【弁理士】

【氏名又は名称】　鈴木　三義

【選任した代理人】

【識別番号】　100106493

【弁理士】

【氏名又は名称】　松冨　豊

【選任した代理人】

【識別番号】　100107836

【弁理士】

【氏名又は名称】　西　和哉

【選任した代理人】

【識別番号】　100108394

【弁理士】

【氏名又は名称】　今村　健一

【選任した代理人】

【識別番号】　100108453

【弁理士】

【氏名又は名称】　村山　靖彦

【選任した代理人】

【識別番号】　100100077

【弁理士】

【氏名又は名称】　大場　充

【手数料の表示】

【予納台帳番号】　008707

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9704954

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　チームデータリスト管理装置及びチームデータリスト保管装置及びチームデータリスト処理システム、並びに、それらの記録媒体

【特許請求の範囲】

【請求項１】　チームを階層化するためのチームデータリストを管理するチームデータリスト管理装置であって、

所定の要求先に前記チームデータリストの操作要求を行い、該操作要求に応じて、操作対象のチームからルートチームに至る各チームについて、自チームの親チームを表す識別子及び前記親チームの管理者の電子署名を含むオーソリティデータと、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名を含むオーソリティリストを有するチームデータリストを前記要求先から取得し、前記識別子を用いて取得されたチームを前記ルートチームまで辿りながら各チームについて、前記チームデータリストの電子署名が改竄されていないこと及び前記管理者情報を用いて権限を持つ者による署名であることを確認して、ユーザによる前記ルートチームのチームマスタの承認を確認する正当性確認手段と、

該正当性確認手段によって正当性が確認された前記チームデータリストに対して前記操作要求に応じた変更を加えるチームデータリスト変更手段と、

前記操作要求を行った指示者の電子署名を作成し、前記変更されたチームデータリストに該電子署名を添付して前記要求先に送出する署名手段と

を具備することを特徴とするチームデータリスト管理装置。

【請求項２】　前記管理者情報は、前記チームマスタにより自チーム内のメンバから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報であることを特徴とする請求項１記載のチームデータリスト管理装置。

【請求項３】　前記ルートチームのチームマスタの本人識別を行うための識別情報を所定の場所から取得して登録する登録手段と、

予め登録されている前記識別情報を用いて、前記要求先から送られてくる前記

ルートチームのオーソリティデータの電子署名が前記チームマスタの電子署名であることを確認するチームマスタ確認手段とをさらに有することを特徴とする請求項１又は２記載のチームデータリスト管理装置。

【請求項４】　チームを階層化するためのチームデータリストを保管するチームデータリスト保管装置であって、

自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータをチーム毎に記憶するオーソリティデータ記憶手段と、

自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストをチーム毎に記憶するオーソリティリスト記憶手段と、

前記オーソリティデータ及び前記オーソリティリストが少なくとも含まれたチームデータリストに対する所定の要求元からの操作要求について、該操作要求の指示者が要求権限を持つことを前記管理者情報を用いて確認するとともに、参照要求或いは削除要求に対して要求されたチームデータリストを前記要求元へ返送し或いは削除し、更新要求に対しては、前記要求元から送られるチームデータリストの電子署名が権限を持つ者による署名であることを前記管理者情報を用いて確認し、前記送られたチームデータリストで前記オーソリティデータ記憶手段及び前記オーソリティリスト記憶手段の記憶内容を更新する権限確認手段と

を具備することを特徴とするチームデータリスト保管装置。

【請求項５】　前記管理者情報は、前記チームマスタにより自チーム内のメンバから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報であることを特徴とする請求項４記載のチームデータリスト保管装置。

【請求項６】　要求元である請求項１～３の何れかの項記載のチームデータリスト管理装置と、

要求先である請求項４又は５記載のチームデータリスト保管装置とを有することを特徴とするチームデータリスト処理システム。

【請求項７】　チームを階層化するためのチームデータリストを管理するチ

ームデータリスト管理プログラムを記録した記録媒体であって、

所定の要求先に前記チームデータリストの操作要求を行う処理と、

前記操作要求に応じて、操作対象のチームからルートチームに至る各チームについて、自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータと、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストを有するチームデータリストを前記要求先から取得する処理と、

前記識別子を用いて取得された各チームを前記ルートチームまで辿りながら各チームについて、前記チームデータリストの電子署名が改竄されていないこと及び前記管理者情報を用いて権限を持つ者による署名であることを確認したのち、ユーザによる前記ルートチームのチームマスタの承認を確認する正当性確認処理と、

該正当性確認処理によって正当性が確認された前記チームデータリストに対して前記操作要求に応じた変更を加える変更処理と、

前記操作要求を行った指示者の電子署名を作成して、前記変更処理によって変更されたチームデータリストに該電子署名を添付して前記要求先に送出する処理と

をコンピュータに実行させるためのチームデータリスト管理プログラムを記録した記録媒体。

【請求項８】　チームを階層化するためのチームデータリストを保管するチームデータリスト保管プログラムを記録した記録媒体であって、

自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータをチーム毎に予め記憶しておく処理と、

自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストをチーム毎に予め記憶しておく処理と、

所定の要求元から前記オーソリティデータ及び前記オーソリティリストが少なくとも含まれたチームデータリストに対する操作要求があったときに、該操作要

求の指示者が要求権限を持つことを前記管理者情報を用いて確認するとともに、該操作要求が参照要求或いは削除要求である場合は、要求されたチームデータリストを前記要求元へ返送し或いは削除し、該操作要求が更新要求である場合は、前記要求元から送られるチームデータリストの電子署名が権限を持つ者による署名であることを前記管理者情報を用いて確認したのち、前記送られたチームデータリストで記憶されている前記オーソリティデータ及び記憶されている前記オーソリティリストを更新する権限確認処理と

をコンピュータに実行させるためのチームデータリスト保管プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、複数のユーザ（メンバ）から構成される企業の部や課といったチームを階層化するためのチームデータリストを作成，管理，保管してゆくとともに、ユーザに提供される各種の情報や様々な機能をユーザ間で安全に共有するためのチームデータリスト処理システムに関するものである。さらに詳細には、チームデータリストの保管に係わる処理を担うチームデータリスト保管装置と、チームデータリスト保管装置上から取得したチームデータリストを対象に様々な管理を行うチームデータリスト管理装置を備えたシステムに関するものである。

【０００２】

【従来の技術】

ユーザに提供される各種の機能や情報といった様々な資源を複数のユーザ間で共有するためには、これら資源にアクセスを要求しているユーザが、本当に資源へアクセスする権利を有しているのか否かを検証する機能を用意しておく必要がある。かかる検証を行うために、従来は、資源に対する正当なアクセス権限を付与されたユーザを予め定義したアクセスコントロールリスト（以下、「ＡＣＬ」と略記する）と呼ばれるリストを利用している。なお、ここで言うＡＣＬは、上述したチームデータリストに含まれる種々の情報のうち、共有資源に対するアクセスを制御するための情報だけが含まれたリストの一例である。

【０００３】

図１５は、ＡＣＬを利用して複数のユーザ間で情報共有を行う従来のシステムの概要を示したものである。同図に示されるシステムでは、イントラネット１，インターネット２がそれぞれファイアウォール３，４を介してサーバ５に接続されており、イントラネット１内部の者ばかりでなく、イントラネット外の共有メンバ６がインターネット２を介して互いに情報を共有している。周知のように、イントラネット１は企業内に整備されたネットワークなどの閉じたネットワークであり、その一方で、インターネット２は世界中にまたがるパブリックなネットワークである。

【０００４】

また、ファイアウォール３，４は悪意を持った侵入者などがイントラネット１へ不正にアクセスすることを防止するためのコンピュータである。サーバ５は各種の資源が蓄積されている端末（コンピュータ）であって、共有情報が格納されたデータベース７と、特定の情報ないし機能にアクセスしても良いグループ及びそれに属するメンバのメンバリストを保持したＡＣＬ８を備えている。このサーバ５は、データベース７に蓄積されている共有情報を管理するデータ保管機能のほか、クライアントに相当する通信相手が予め許可されている者か否かを検証するユーザ認証機能，ＡＣＬ８に基づいて共有情報に対するアクセスの可否を検証するアクセス制御機能，ＡＣＬ８に基づいて特定のグループに属するメンバだけが特定の共有情報へアクセスすることを可能ならしめるグループ管理機能を備えている。

【０００５】

図１５のシステムでは、共有メンバ６やイントラネット１内部のユーザからデータベース７に対するアクセス要求があると、サーバ５はその都度ＡＣＬ８を参照してユーザ認証を行い、当該ユーザがメンバとしてＡＣＬ８に定義されていればアクセスを許可し、メンバとして定義されていなければアクセスを拒否する。また、当該ユーザに対してアクセスが許可されている場合、サーバ５はＡＣＬ８を参照して当該メンバが特定のグループに含まれるかどうかを確認するとともに、当該メンバがアクセス要求のある共有情報に関してアクセスを許されているか

どうか調べるようにしている。

【０００６】

【発明が解決しようとする課題】

ところで、複数のユーザ間で資源を共有する場合にはサーバ側の管理者を共有メンバに含めるのが好ましくない場合もある。例えば、ある企業の情報システム部に所属するシステム管理者は、人事部内だけで共有すべき企業の人事情報にアクセス不可能であることが必要と考えられる。ところが、上述した図１５のようなシステムでは、サーバ５の管理者に対してＡＣＬ８の設定や管理を行う権限を許与してしまっている。そのため、サーバ管理者５がＡＣＬ８に対して不正なアクセスを行うことが可能であり、意図的にＡＣＬ８の設定内容が改竄されるのを防止することができない欠点がある。これに加えて、サーバ管理者以外にも、サーバＳＶへ不正に侵入する者（いわゆるクラッカ）によってＡＣＬ８が不正に改竄されてしまうおそれもある。

【０００７】

このほか、企業内部で情報を共有してゆく利用形態などへの適用を考えた場合、そうした形態にうまく適合したシステムを構築してゆくことが望ましい。すなわち、ある程度以上の規模の企業では組織がピラミッド状に形成された階層関係になっており、例えば、人事部の配下には人事一課や人事二課が設置されていることなどはごく一般的であると言える。また、開発部門などでは商品の開発工程などに合わせて例えば開発部長が新たに課を作ったり、幾つかの課を統合したり、あるいは、ある特定の課を廃止したりする権限が与えられている場合も考えられる。また、それぞれの課が業務別にいくつかのグループに分かれていることもある。

【０００８】

そうした組織にあっては、開発部長が各課やそれぞれの課に属する全てのグループの構成員を管理することは非常な負担である。そこで、こうした管理負担を分散するために、開発部長を補佐する者を何人か割り当てるようにしてこれらの者に管理業務の一部又は全部を代行させることなどが行われている。さらには、開発部長には課の作成，統廃合等の業務を行う権限だけを与えておき、課内部の

管理や情報共有自体は課長やその下のグループリーダ等に一任するといった形態が採られている。しかるに、上述した従来のシステムではいま説明したような企業の組織形態に適合した柔軟な管理や情報共有は何ら考慮されていないという問題がある。

【０００９】

本発明は上記の点に鑑みてなされたものであり、その目的は、サーバの管理者といった特権者も含め、企業の組織単位等に相当するチームの外にいる者，クラッカ等がチームデータリストに不正を行うことを防止しつつ、チームの階層化および各種の情報や機能の実現するためのチームデータリスト処理システムを提供することにある。さらに詳しくは、各チームに所属しているメンバから特に選ばれた者だけが、チームの配下にサブチームを作成したり、サブチームの作成権限を特定の複数人に割り当てたり、サブチームの作成権限者が選定した特定人にサブチーム内の管理を行わせたりすることが可能なチームデータリスト処理システムを提供することにある。

【００１０】

【課題を解決するための手段】

以上の課題を解決するために、請求項１記載の発明は、チームを階層化するためのチームデータリストを管理するチームデータリスト管理装置であって、所定の要求先に前記チームデータリストの操作要求を行い、該操作要求に応じて、操作対象のチームからルートチームに至る各チームについて、自チームの親チームを表す識別子及び前記親チームの管理者の電子署名を含むオーソリティデータと、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名を含むオーソリティリストを有するチームデータリストを前記要求先から取得し、前記識別子を用いて取得されたチームを前記ルートチームまで辿りながら各チームについて、前記チームデータリストの電子署名が改竄されていないこと及び前記管理者情報を用いて権限を持つ者による署名であることを確認して、ユーザによる前記ルートチームのチームマスタの承認を確認する正当性確認手段と、該正当性確認手段によって正当性が確認された前記チームデータリストに対して前記操作要

求に応じた変更を加えるチームデータリスト変更手段と、前記操作要求を行った指示者の電子署名を作成し、前記変更されたチームデータリストに該電子署名を添付して前記要求先に送出する署名手段とを具備することを特徴としている。

【００１１】

また、請求項２記載の発明は、請求項１記載の発明において、前記管理者情報は、前記チームマスタにより自チーム内のメンバから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報であることを特徴としている。

また、請求項３記載の発明は、請求項１又は２記載の発明において、前記ルートチームのチームマスタの本人識別を行うための識別情報を所定の場所から取得して登録する登録手段と、予め登録されている前記識別情報を用いて、前記要求先から送られてくる前記ルートチームのオーソリティデータの電子署名が前記チームマスタの電子署名であることを確認するチームマスタ確認手段とをさらに有することを特徴としている。

【００１２】

また、請求項４記載の発明は、チームを階層化するためのチームデータリストを保管するチームデータリスト保管装置であって、自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータをチーム毎に記憶するオーソリティデータ記憶手段と、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストをチーム毎に記憶するオーソリティリスト記憶手段と、前記オーソリティデータ及び前記オーソリティリストが少なくとも含まれたチームデータリストに対する所定の要求元からの操作要求について、該操作要求の指示者が要求権限を持つことを前記管理者情報を用いて確認するとともに、参照要求或いは削除要求に対して要求されたチームデータリストを前記要求元へ返送し或いは削除し、更新要求に対しては、前記要求元から送られるチームデータリストの電子署名が権限を持つ者による署名であることを前記管理者情報を用いて確認し、前記送られたチームデータリ

ストで前記オーソリティデータ記憶手段及び前記オーソリティリスト記憶手段の記憶内容を更新する権限確認手段とを具備することを特徴としている。

また、請求項５記載の発明は、請求項４記載の発明において、前記管理者情報は、前記チームマスタにより自チーム内のメンバから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報であることを特徴としている。

また、請求項６記載の発明は、要求元である請求項１～３の何れかの項記載のチームデータリスト管理装置と、要求先である請求項４又は５記載のチームデータリスト保管装置とを有することを特徴としている。

【００１３】

また、請求項７記載の発明は、チームを階層化するためのチームデータリストを管理するチームデータリスト管理プログラムを記録した記録媒体であって、所定の要求先に前記チームデータリストの操作要求を行う処理と、前記操作要求に応じて、操作対象のチームからルートチームに至る各チームについて、自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータと、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストを有するチームデータリストを前記要求先から取得する処理と、前記識別子を用いて取得された各チームを前記ルートチームまで辿りながら各チームについて、前記チームデータリストの電子署名が改竄されていないこと及び前記管理者情報を用いて権限を持つ者による署名であることを確認したのち、ユーザによる前記ルートチームのチームマスタの承認を確認する正当性確認処理と、該正当性確認処理によって正当性が確認された前記チームデータリストに対して前記操作要求に応じた変更を加える変更処理と、前記操作要求を行った指示者の電子署名を作成して、前記変更処理によって変更されたチームデータリストに該電子署名を添付して前記要求先に送出する処理とをコンピュータに実行させることを特徴としている。

【００１４】

また、請求項８記載の発明は、チームを階層化するためのチームデータリストを保管するチームデータリスト保管プログラムを記録した記録媒体であって、自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータをチーム毎に予め記憶しておく処理と、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストをチーム毎に予め記憶しておく処理と、所定の要求元から前記オーソリティデータ及び前記オーソリティリストが少なくとも含まれたチームデータリストに対する操作要求があったときに、該操作要求の指示者が要求権限を持つことを前記管理者情報を用いて確認するとともに、該操作要求が参照要求或いは削除要求である場合は、要求されたチームデータリストを前記要求元へ返送し或いは削除し、該操作要求が更新要求である場合は、前記要求元から送られるチームデータリストの電子署名が権限を持つ者による署名であることを前記管理者情報を用いて確認したのち、前記送られたチームデータリストで記憶されている前記オーソリティデータ及び記憶されている前記オーソリティリストを更新する権限確認処理とをコンピュータに実行させることを特徴としている。

【００１５】

【発明の実施の形態】

以下、図面を参照して本発明の実施形態について説明するが、まず初めに本発明におけるチームデータリストについて説明する。本発明におけるチームデータリストは、チームに関する情報を定義したリストの総称であって、上述したＡＣＬのような機密性の高い管理が要求される用途に適用される「メンバの集合」を定義するためのものである。上述した通り、従来のシステムでは、チームのメンバではない端末管理者，ネットワーク管理者，サーバ管理者などがチームに関する情報を変更することができる。一方、本発明におけるチームデータリストでは、チームに関する情報を複数のリスト（後述するようなオーソリティリスト，オーソリティデータやメンバリスト，チームマスタリスト，アプリケーションリスト）に分割して管理することで、チームの階層化やチームマスタ自身の変更といったチーム管理をチーム内のメンバだけで行えるようにしている。

【００１６】

以下に詳述する実施形態では、第一に、チームの配下にサブチームを作成できるようにして、会社組織等における階層関係を模擬して情報共有を行ってゆく仕組みを実現している。第二には、特に選定された複数の人間に対してサブチームの作成権限を授与できるような仕組みを実現しており、それによって一人の管理者に負荷が集中しないようにして管理負担の分散を図っている。第三には、サブチーム内部の管理については、サブチーム作成権限者がサブチーム内から選んだ特定の者に行わせる仕組みを実現している。そうすることによって、チームの管理者がサブチーム内部の管理や情報共有に関与しなくとも済むようにしている。

【００１７】

〔第１実施形態〕

本実施形態では、階層化されたチームに合わせて、チームデータリストにアクセスできる者をその権限の内容に応じてメンバ，サブオーソリティ，チームマスタの３種類に分類しており、この順番でその者に付与される権限が拡大してゆく。チームマスタは或るチームの管理者であって、当該チームの配下の組織たるサブチームの作成といった管理権限を有する者である。一方、サブオーソリティはチームマスタによって指名された者であって、チームマスタと同様にサブチームの作成といった管理権限を持つ者であるが、他の者をサブオーソリティとして指名することは許されていない。サブオーソリティは複数人いる場合もあれば一人もいない場合もある。他方、サブオーソリティ及びチームマスタ以外の一般のメンバは情報や機能を共有する者であって、サブチームの作成権限などの特権はいっさい与えられていない。なお、サブオーソリティやチームマスタは特別な権限が与えられてはいるが、チーム内のメンバであることに変わりはなく、その意味でサブオーソリティやチームマスタをメンバと呼ぶこともある。なお、以下の説明及び図面ではチームマスタを「ＴＭ」と略記し、サブオーソリティを「ｓｕｂＡＵ」と略記することがある。

【００１８】

以下、チームデータリスト管理装置及びチームデータリスト保管装置の２つの装置を備えたシステムについて本実施形態を説明してゆく。図１は、チームデー

タリスト管理装置及びチームデータリスト保管装置を具備した本実施形態のシステム全体の構成を示したブロック図である。同図において、チームデータリスト管理装置３０，チームデータリスト保管装置３１は以下に詳述するチームデータリスト管理機能，チームデータリスト保管機能をそれぞれ備えており、互いに通信機能を利用してデータを授受している。チームデータリスト管理装置３０，チームデータリスト保管装置３１は何れもワークステーションなどの一般的なコンピュータで実現することが可能であり、これらコンピュータの主記憶上にはそれぞれチームデータリスト管理機能，チームデータリスト保管機能を実現するためのプログラム（チームデータリスト管理プログラム，チームデータリスト保管プログラム）が記憶される。

【００１９】

これらのプログラムはフロッピーディスク，ＩＣ（集積回路）カード，光磁気ディスク，ＣＤ－ＲＯＭ（コンパクトディスク－読み取り専用メモリ）等の可搬性のある記憶媒体や、コンピュータに内蔵されるハードディスクなどの大容量の記憶媒体といったコンピュータ読み取り可能な記憶媒体にその一部又は全部が記憶されている。すなわち、当該プログラムは以下に詳述する機能の一部を実現するためのものであっても良く、さらにはコンピュータにすでに記録されているプログラムとの組み合わせでこれら機能を実現できるものであっても良い。そして、チームデータリスト管理装置やチームデータリスト保管装置を作動させるにあたって、これらのプログラムがコンピュータ上のＣＰＵ（中央処理装置）の指示の下に予め記憶媒体から主記憶上に転送される。その後、ＣＰＵは主記憶上に転送されたプログラムを実行し、それによって装置各部を制御して、以下に詳述する様々な処理を実現している。

【００２０】

なお、ここで言う「コンピュータ」にはＯＳ（オペレーティングシステム）や周辺機器等のハードウェアが含まれている。また、コンピュータ読み取り可能な記憶媒体としてはいま述べたようなプログラムを静的に記憶するものに限られるものではなく、専用線や電話回線などの通信回線を通じて短時間だけ動的にプログラムを保持するもの，即ち、インターネット等のネットワークでプログラムや

データを保持，転送，中継するサーバ，ルータ，ゲートウェイといったコンピュータ機器に内蔵された主記憶やキャッシュメモリ、サーバ，クライアントとして機能するコンピュータ内部の揮発性メモリなどのように、一定時間プログラムを保持可能なものをすべて包含している。

【００２１】

さて、図１に示すチームデータリスト保管装置３１にはハードディスク等のデータベースを構築可能な記憶装置３２が接続されている。この記憶装置３２は、複数のメンバで構成されるチーム毎にオーソリティデータ３３とオーソリティリスト３４からなるチームデータリストの組を記憶している。同図では説明の都合からオーソリティデータ３３及びオーソリティリスト３４の組を一つだけ示しているが、実際にはチームの数だけこれらの組が存在している。ここで、図２（ａ），（ｂ）はオーソリティデータ３３，オーソリティリスト３４の詳細な構造を示したものである。また、同図（ｃ），（ｄ）はこれ以後に掲げる図面中において、オーソリティデータ３３，オーソリティリスト３４の記憶内容を簡略化して示すための表記法をそれぞれ示したものである。なお、以下の説明及び図面ではオーソリティデータを「ＡＵＤ」と略記し、オーソリティリストを「ＡＵＬ」と略記することがある。

【００２２】

オーソリティデータ３３は或るチームとその配下のサブチームとの関係を表すデータであって、サブチームとの関係において上位にある当該チームを親チームと呼ぶ。図２（ａ）に示すように記号“ＡＵＤ”がオーソリティデータであることを示しており、このオーソリティデータ３３は、自身のチームに付与された識別子たるチームＩＤ３３ａ，このチームの親チームに付与されたチームＩＤである親チームＩＤ３３ｂ，親チームの誰がこのチームを作成したかを意味するチーム作成者３３ｃ，このチームに属するメンバの誰に対してチームマスタ権限を与えたかを示すチームマスタ３３ｄ，チーム作成者３３ｃのデジタル署名（電子署名とも言う）がなされる署名３３ｅを含んでいる。また、図２（ｃ）において、このオーソリティデータはチーム１０１のサブチームであるチーム１０２に関するものであることが分かる。これに加えて、デジタル署名からこのオーソリティ

データのチーム作成者がメンバＢであることが分かるほか、チームマスタがメンバＸであることが分かる。

【００２３】

一方、オーソリティリスト３４は各チームにおける複数の管理者を登録したリストであって、当該チームのチームマスタやサブオーソリティに関するデータが含まれている。図２（ｂ）に示すように記号“ＡＵＬ”がオーソリティリストを意味しており、このオーソリティリスト３４はこのチームに関するチームＩＤ３４ａ，チームマスタ３４ｂ，サブオーソリティ３４ｃ（同図の場合は二人），チームマスタ３４ｂのデジタル署名たる署名３４ｄを含んでいる。そして、図２（ｄ）によれば、チームマスタがメンバＸであってその署名がなされているほか、サブオーソリティがメンバＣ及びメンバＤであることが分かる。なお、同図（ｄ）ではチームＩＤの表記自体は省略されている。以上のように、本実施形態によるチームデータリストは、親チーム及びサブチームの関係を示すリストであるＡＵＤと、サブチーム管理に関わるリストであるＡＵＬに分割された構造となっている。

【００２４】

なお、オーソリティデータ３３やオーソリティリスト３４には、図２に示した以外にも、これらデータやリストの作成時間を示すタイムスタンプ，署名３３ｅや署名３４ｄを作成するのに用いられる署名アルゴリズム，オーソリティデータ３３やオーソリティリスト３４自身の有効期限，オーソリティデータ３３やオーソリティリスト３４自身の識別番号に関するデータなどを含んでいる。また、メンバ，サブオーソリティ，チームマスタの各個人を識別するためのＩＤ（識別子）としては、名前，メールアドレス，組織上の名称，個人のシリアルナンバ，デジタル証明書等、種々のものを用いることが可能である。

【００２５】

次に、図３は階層化されたチームの概念図についてその一例を示したものである。同図に示されるように、チームの階層はコンピュータのファイルシステムのように木構造になっており、図中の楕円形がチームを表現するとともに、親チームとそのサブチームが直線で互いに結ばれている。各チームには複数のサブチー

ムを登録することができ、例えば人事部のチームの配下に人事一課，人事二課などのサブチームを登録することが可能になっている。また、頂点に存在するチーム１０１は木構造の根に相当しているため、ファイルシステム上のルートディレクトリになぞらえて本実施形態では「ルート（Ｒｏｏｔ）」ないしルートチームと呼んでいる。さらに、チーム１０２及びチーム１０３は何れもチーム１０１のサブチームであって、木の上では同じ階層に属するチームである。一方、チーム１０４はチーム１０３のサブチームである。

【００２６】

一方、図４は図３に示したチーム階層に対応させて各チームのオーソリティリストやオーソリティデータについて具体的な値を記入したものである。なお、同図ではオーソリティリスト及びオーソリティデータの他に、互いに情報や機能を共有する共有メンバの一覧を示したメンバリスト（図中の「ＭＬ」）が各チームに含まれている例を示してある。つまり、この図においては、チームデータリストがオーソリティリスト，オーソリティデータ，メンバリストの３種類のリストで構成される。各メンバリスト１０１ｍ～１０４ｍにはメンバリストの作成者の署名とメンバの一覧が図示されているが、これ以外にも、チームの利用目的に合致した様々なチームの管理情報が含まれている。すなわち、各メンバの識別情報，各メンバに付与された公開鍵方式における公開鍵（即ち、所定長のビット列）とこの公開鍵に対応する保有者の識別子（以下、「公開鍵ＩＤ」という），チームＩＤ，メンバリストの作成時間を示すタイムスタンプ，チーム内のメンバが利用できる機能（例えば、アプリケーション）に関する情報などが含まれている。このほか、それぞれのメンバリストには各メンバに関する情報として、ｅ－ｍａｉｌ（電子メール）アドレスやメンバ自身の住所といった情報も含まれており、これらを用いることで各メンバに関する情報リソースの管理も同時に行うことができる。

【００２７】

同図に示す構成によれば、オーソリティデータに記述された親チームＩＤを辿ってゆくことで、何れのサブチームからもルートたるチーム１０１に到達することができる。このほか、各チームでは複数の管理者がサブチームを作成可能であ

る。例えばチーム１０１ではチームマスタＡ及びサブオーソリティＢ，Ｃがサブチームの作成権限を有しており、オーソリティデータ１０２ｄ，１０３ｄの署名から分かるように、サブチームたるチーム１０２，１０３はそれぞれチーム１０１のサブオーソリティＢ，Ｃが作成している。

【００２８】

あるサブチームのオーソリティデータは当該サブチームの親チームに登録された管理者が作成することになっている。また、当該サブチーム内の誰もが親チームの管理者の指示によってこのサブチームのチームマスタになることができる。例えばチーム１０４では、オーソリティデータ１０４ｄのデジタル署名がメンバＶであるから、親であるチーム１０３の管理者の一人であるサブオーソリティＶがオーソリティデータ１０４ｄを作成しており、チーム１０４のチームマスタとしてメンバＬを指名している。

【００２９】

一方、オーソリティリストは各チームのチームマスタが作成して署名することになっている。例えば、チーム１０３のオーソリティリスト１０３ｕはチームマスタたるメンバＸが作成したものであって、そこにはメンバＸのデジタル署名がなされている。そのため、オーソリティリスト１０３ｕ中のサブオーソリティに関するデータはメンバＸのみが管理できることになり、親チームたるチーム１０１の管理者（即ち、チームマスタＡやサブオーソリティＢ，Ｃ）の干渉を受けることはない。換言するならば、オーソリティリストの署名者をチームの作成者（即ち、親チームのチームマスタやサブオーソリティ）にしてしまうと、例えば人事部長が人事課長に課内部の管理を任せることができなくなって自分で管理してゆかねばならなくなる。同様にして、メンバリストの署名についても各チームのチームマスタが行うことから、各チーム内の共有メンバに関する管理についても親チームの干渉を受けずに済むことになる。例えばチーム１０３のメンバリスト１０３ｍはチームマスタＸが署名しているため、親チームの管理者が管理することはできない。ただし、サブチームを最初に作成したときの初期状態や、サブチームのチームマスタを親チームのチームマスタやサブオーソリティが変更した場合には、オーソリティリストの署名は、該サブチームを作成した親チームのチー

ムマスタ又はサブオーソリティの署名となっている。

【００３０】

以上の点をまとめると、本実施形態ではオーソリティデータとオーソリティリストを分離する構成としており、親チームはサブチームのオーソリティデータＡＵＤを参照することができる一方、親チームの管理者がオーソリティリストやメンバリストを改竄できないようにすることで、サブチーム内部の管理に親チームは関与しないようにしている。これによって、各チームのチームマスタは、自分でサブオーソリティを選択できるほか、チーム内の情報共有のメンバ管理も行うことができる。

【００３１】

次に、図１のチームデータリスト保管装置３１において、権限確認機能３５はクライアントＣＬ側からオーソリティデータ３３やオーソリティリスト３４に対する参照，変更，削除の各要求があったときに、要求者を識別してこれらの要求を許可するのか拒否するのかを判断する。この判断にあたっては、要求対象となっているチームのチームマスタ，サブオーソリティや当該チームの親チームやサブチームとの間の関係のほか、チームに所属するメンバ等の権限と要求者本人に与えられている権限などを照らし合わせている。つまり、要求内容によって判断手順の詳細が異なるためその詳細については後述する動作説明に譲る。次に、リスト保管機能３６は権限確認機能３５がオーソリティデータ３３やオーソリティリスト３４を使用するにあたって、これらのリストを記憶装置３２から取得し，記憶装置３２から削除し，あるいは記憶装置３２へ保存する処理を司っている。以下の説明では、権限確認機能３５がオーソリティデータ３３やオーソリティリスト３４にアクセスする場合には必ずリスト保管機能３６が介在することを前提としているが、煩雑になるため一々説明しない。

【００３２】

次に、チームデータリスト管理装置３０において、リスト正当性確認機能３７はルートチームに至るまで親チームのオーソリティリスト及びオーソリティデータを順次辿ってゆき、最終的にチーム１０１のチームマスタＡの署名を確認してオーソリティリスト及びオーソリティデータの正当性を検証している。なお、こ

こで言う正当性とは改竄や越権行為などが無く正当な手順を経てチーム階層の管理が行われていることを意味している。次に、ＡＵＤ・ＡＵＬ変更機能３８は、リスト正当性確認機能３７が取得したオーソリティデータ３３やオーソリティリスト３４に対してメンバや管理者の追加，削除，置換などの変更を加えるほか、サブチーム作成時などではオーソリティデータ３３及びオーソリティリスト３４を新たに作成することもある。次いで、電子署名機能３９はＡＵＤ・ＡＵＬ変更機能３８によって処理がなされたオーソリティデータ３３やオーソリティリスト３４に対し、変更者本人しか知り得ない秘密鍵ないし署名鍵を用いた暗号とハッシュ関数とを併用してこれらリストの作成者ないしは変更者（即ち、チームマスタ又はサブオーソリティ）のデジタル署名を付加する。

【００３３】

次に、公開鍵管理機能４０は、チームデータリスト管理装置３０に接続された公開鍵データベース４１にアクセスして、公開鍵と当該公開鍵に対応する公開鍵ＩＤを取得する。ちなみに、実際の形態において、公開鍵データベース４１はチームデータリスト管理装置３０に直接的に接続されたローカルな形態のみならず、インターネット等のネットワーク上に設置されたサーバ（例えば、認証局）に存在している形態も当然に考えられる。こうした形態によれば、公開鍵管理機能４０は認証局上に登録されたホームページを介して公開鍵データベース４１にアクセスし、そこから上述した公開鍵及び公開鍵ＩＤをファイルの形式で取得することも可能となる。

【００３４】

次に、上記構成によるチームデータリスト管理装置３０およびチームデータリスト保管装置３１を有するシステムの動作についてクライアントＣＬからサーバＳＶに対して為される要求内容毎に説明してゆく。

【００３５】

〔サブチームの作成〕

図５はサブチームを作成するための処理手順を示している。ここでは図４に示したチーム１０１のサブオーソリティであるメンバＣが、チーム１０１の配下にチームマスタをメンバＸとしたサブチーム１０３を作成するものとする。これは

、人事部長の代行として部長代理が人事部の下に課を新設する業務を遂行する場合などに相当する。ここで、チームデータリスト保管装置３１では正当な手順に従って作成されたチーム１０１に関するチームデータリストが予め記憶装置３２上に格納されており、ルートチーム１０１のチームマスタＡによる管理体系でサブチームの作成が行われる。なお、図４に示したように、チーム１０１には親チームは存在しないのでオーソリティデータ１０１ｄの親チームＩＤには固定値「Ｒｏｏｔ」が設定されているほか、チームマスタはメンバＡであるためオーソリティデータ１０１ｄ及びオーソリティリスト１０１ｕには何れもメンバＡのデジタル署名がされている。もっとも、ルートチームには仮想的に「Ｒｏｏｔ」という親チームがあると見なすことができ、また、この親チームがチームマスタとしてメンバＡを指名していると見なすことができる。

【００３６】

まず、メンバＣからのサブチーム作成指示に従って、チームデータリスト管理装置３０がサブチーム作成要求をチームデータリスト保管装置３１に送出する（ステップＳ１１）。チームデータリスト保管装置３１は記憶装置３２からオーソリティデータ１０１ｄ及びオーソリティリスト１０１ｕを取得して、これらをチームデータリスト管理装置３０に送出する。その際、チームデータリスト保管装置３１はチーム１０１の配下にサブチーム（即ち、図４に示すチーム１０２）があればそれらチームに関するチームデータリストも併せてチームデータリスト管理装置３０へ送出する（ステップＳ１２）。チームデータリスト管理装置３０では、ＡＵＤ・ＡＵＬ変更機能３８がメンバＣからの指示に基づいて、親チームＩＤをチーム１０１，チームＩＤをチーム１０３，チームマスタをメンバＸとしたオーソリティデータ１０３ｄを作成するとともに、チームマスタをメンバＸとしたオーソリティリスト１０３ｕａを作成する。次に、ＡＵＤ・ＡＵＬ変更機能３８は作成したオーソリティリスト１０３ｕａをオーソリティデータ１０３ｄと一緒にして電子署名機能３９に引き渡す。

【００３７】

電子署名機能３９は、秘密鍵ファイルや秘密鍵の記録されたＩＣカード等からメンバＣに関する秘密鍵を取得し、これを基にＡＵＤ・ＡＵＬ変更機能３８から

送られたオーソリティデータ１０３ｄ及びオーソリティリスト１０３ｕａに対して要求者たるメンバＣのデジタル署名を行う。この時点ではオーソリティリスト１０３ｕａの署名はチームマスタＸのものではなく、サブチーム作成者の署名になっている（以上、ステップＳ１３）。次に、電子署名機能３９は、チーム１０３について作成されたオーソリティデータ１０３ｄ及びオーソリティリスト１０３ｕａをチームデータリスト保管装置３１に送出して、これらの保存要求を行う（ステップＳ１４）。

【００３８】

チームデータリスト保管装置３１では、権限確認機能３５が図６のフローチャートに示される権限確認を行う。まず、権限確認機能３５は保存要求を行った要求者がメンバＣであることを識別（ステップＳ３１）し、チーム１０１に関するオーソリティデータ１０１ｄ及びオーソリティリスト１０１ｕを基に、メンバＣがチーム１０１のチームマスタ又はサブオーソリティであるかどうか調べる（ステップＳ３２）。この場合、メンバＣはチーム１０１のサブオーソリティであるため、正当な権限を持つ者によって作成されたデータの保存要求と判断（同ステップの判断結果が“ＹＥＳ”）する。ちなみに、同ステップの判断結果が“ＮＯ”となる場合には改竄ないしは不正行為が存在しているため、権限確認機能３５は要求された保存動作を行うことなく処理を中止する。

【００３９】

次に、権限確認機能３５は作成されたサブチーム１０３のオーソリティデータ１０３ｄ及びオーソリティリスト１０３ｕａの署名がともに要求者たるメンバＣのものであることを確認する（ステップＳ３３）。この場合は、前述したように何れもメンバＣが署名しているため同ステップの判断結果は“ＹＥＳ”となり、権限確認機能３５は正常な権限でサブチームが作成されたものと最終的に判断して、作成されたサブチームのオーソリティデータ１０３ｄとオーソリティリスト１０３ｕａを記憶装置３２に保存する（ステップＳ３４）。ちなみに、ステップＳ３３の判断結果が“ＮＯ”となる場合には改竄ないしは不正行為が存在しているため、権限確認機能３５は要求された保存動作を行うことなく処理を中止する（なお、以上の処理は図５のステップＳ１５に相当）。以上の手順によってサブ

チームの作成が完了する。

【００４０】

この後、チーム１０３のチームマスタたるメンバＸから当該チームに対して、情報共有のメンバやサブチーム作成権限者の設定といった管理要求があったものとする。なお、ここでは一事例としてチーム１０３のサブオーソリティとしてメンバW及びメンバＶを新たに登録する場合について説明する。図５に示すように、まずチームデータリスト管理装置３０は、メンバＸから指示された管理要求に基づいて、親チーム１０３に関するチームデータリストをチームデータリスト保管装置３１に要求する（ステップＳ１６）。すると、チームデータリスト保管装置３１は要求内容をもとにしてサブチーム１０３のほかルートチームに至るまでの全ての親チーム（この場合はルートチームたるチーム１０１のみ）に関するチームデータリストをそれぞれチームデータリスト管理装置３０側に転送する（ステップＳ１７）。チームデータリスト管理装置３０では、リスト正当性確認機能３７が図７のフローチャートに示される処理手順に従って、転送されてきたリストの正当性を調べる（ステップＳ１８）。

【００４１】

まず、リスト正当性確認機能３７は、管理対象であるチーム１０３のオーソリティデータ１０３ｄ及びオーソリティリスト１０３ｕａのデジタル署名を参照してそれらが改竄されているかどうか確認（ステップＳ４１）し、改竄があれば不正行為があったものとして管理要求に関わる処理を中止する（同ステップの判断結果が“ＮＯ”）。一方、同ステップの判断結果が“ＹＥＳ”であって改竄がなければ、リスト正当性確認機能３７は、オーソリティデータ１０３ｄからメンバＸがチーム１０３のチームマスタであることを確認できる。ここで、通常であれば、リスト正当性確認機能３７はオーソリティリスト１０３ｕａからその署名者がチームマスタたるメンバＸであることを確認する。しかし、前述したようにこの時点はサブチーム作成途上の過渡期になっており、オーソリティリスト１０３ｕａの署名者がサブチーム作成者であるメンバＣになっているので、メンバＣがサブチームを作成する正当な権利を持っているかどうかは、後述する処理（ステップＳ４５）で、メンバＣが親チーム１０１のチームマスタもしくはサブオーソ

リティとして登録されているか調べることで確認する（ステップＳ４２）。

【００４２】

次に、リスト正当性確認機能３７はオーソリティデータ１０３ｄの親チームＩＤから親チームがチーム１０１であることを知り（ステップＳ４３）、親チームのオーソリティデータ１０１ｄ及びオーソリティリスト１０１ｕのデジタル署名が改竄されているかどうか調べる（ステップＳ４４）。そしてこれらの何れかでも改竄されていれば、不正行為があったとしてリスト正当性確認機能３７は処理を中止する（同ステップの判断結果が“ＮＯ”）が、同ステップの判断結果が“ＹＥＳ”であって改竄がなければ、引き続いてチーム１０３の作成者が親チームのチームマスタ又はサブオーソリティであるかどうかを確認する（ステップＳ４５）。この場合、チーム１０３のオーソリティデータ１０３ｄの署名者はメンバＣであり、また、親であるチーム１０１のオーソリティリスト１０１ｕからメンバＣが親チームのサブオーソリティとして登録されていることが分かり、チーム１０３が正当な作成権限を持つ者によって作成されていることが確認できる（同ステップの判断結果が“ＹＥＳ”）。なお、同ステップの判断結果が“ＮＯ”であれば、リスト正当性確認機能３７は不正行為があったものとして処理を中止する。

【００４３】

次に、リスト正当性確認機能３７は親であるチーム１０１がルートであるかどうか調べるが、この場合はチーム１０１のオーソリティデータ１０１ｄの親チームＩＤが“Ｒｏｏｔ”であることからルートチームであることが分かる（ステップＳ４６の判断結果が“ＹＥＳ”）。そこで、リスト正当性確認機能３７はチーム１０１のオーソリティデータ１０１ｄを調べることでそのチームマスタがメンバＡであることが分かる。そして、このメンバＡによってオーソリティデータ１０１ｄ及びオーソリティリスト１０１ｕが署名されていることから、チーム階層がチームマスタＡの下で正当に管理されていることを確認できる（ステップＳ４７）。最後に、メンバＸ自身がチームデータリスト管理装置３０を操作して、ルートチーム１０１のチームマスタＡが管理するチーム階層の下に、情報共有などのチームデータリストの利用や階層化されたチームの利用が為されていることを

承認して、この旨をリスト正当性確認機能３７に通知する。

【００４４】

以上の手順により、リスト正当性確認機能３７は、チーム１０１のチームマスタＡの指名したサブオーソリティＣがチーム１０３に関するオーソリティデータ及びオーソリティリストを作成しており、チームデータリスト保管装置３１から正常な状態でこれらチームデータリストが取得されていることを確認できる。そこで、リスト正当性確認機能３７はチームデータリスト保管装置３１から転送されたチームデータリストをＡＵＤ・ＡＵＬ変更機能３８に渡す。なお、図７のステップＳ４６で親チームがルートチームと判断されなかった場合、例えばチーム１０３のサブチームであるチーム１０４に対して管理要求を行った場合、リスト正当性確認機能３７は対象とするチームを親チームに変更してチーム階層をルートチームに向かって一つ上がり（ステップＳ４９）、親チームがルートチームたるチーム１０１になる（ステップＳ４６の判断結果が“ＹＥＳ”）までステップＳ４２～Ｓ４６及びステップＳ４９から成るループを繰り返して実行する。

【００４５】

次に、ＡＵＤ・ＡＵＬ変更機能３８はチーム１０３のオーソリティリスト１０３ｕａに対して、サブオーソリティとしてメンバW及びメンバVを加えたオーソリティリスト１０３ｕを作成し、これをオーソリティデータ１０３ｄとともに電子署名機能３９に渡す。電子署名機能３９は前述した秘密鍵ファイル等からチームマスタXに関する秘密鍵を取得し、渡されたオーソリティリスト１０３ｕに対してチームマスタXの署名を行ったのち（以上、ステップＳ１９）、これをオーソリティデータ１０３ｄとともにチームデータリスト保管装置３１に転送してこれらチームデータリストに関する保存要求を行う（ステップＳ２０）。

【００４６】

チームデータリスト保管装置３１において、権限確認機能３５はチームデータリスト管理装置３０からの保存要求に対し、記憶装置３２に保管されているチーム１０１に関わるチームデータリストとクライアント側から転送されてくるチーム１０３に関わるチームデータリストに基づいて、図８のフローチャートで示される権限確認を行う。すなわち、まず権限確認機能３５は保存要求を指示した要

求者がメンバＸであることを識別（ステップＳ５１）し、転送されてきたオーソリティデータ１０３ｄ及びオーソリティリスト１０３ｕをもとにして、上記要求者が、チーム１０３のチームマスタ，親であるチーム１０１のチームマスタ又はサブオーソリティの三者のうち何れかに一致するかどうかを確認する。この場合は要求者たるメンバＸがチーム１０３のチームマスタとして登録されている（ステップＳ５２の判断結果が“ＹＥＳ”）ので、権限確認機能３５は要求者が保存要求に対する正当な権限を持っていると判断する。ちなみに、同ステップの判断結果が“ＮＯ”であれば、権限確認機能３５は要求者に正当な権限が与えられていないものとして処理を中止する。

【００４７】

次に、権限確認機能３５はオーソリティデータ１０３ｄの署名者が親チームのチームマスタ又はサブオーソリティの何れかに一致するかどうか確認する。この場合、オーソリティデータ１０３ｄの署名者はメンバＣであって親チーム１０１のサブオーソリティである（ステップＳ５３の判断結果が“ＹＥＳ”）ため、権限確認機能３５は要求者が保存要求に対する正当な権限を持っていると判断する。ちなみに、同ステップの判断結果が“ＮＯ”であれば、権限確認機能３５は改竄や不正行為があったものとして処理を中止する。次に、権限確認機能３５は、オーソリティリスト１０３ｕの署名者がオーソリティデータ１０３ｄに登録されているチームマスタと一致するかどうかを確認する。この場合、オーソリティリスト１０３ｕの署名者はオーソリティデータ１０３ｄの示すチームマスタＸである（ステップＳ５４の判断結果が“ＹＥＳ”）ことから、権限確認機能３５は正常な権限を持つ者によってチーム１０３が作成されたものと最終判断を下して、チームデータリスト管理装置３０から転送されたチームデータリストを記憶装置３２に保存して、チーム１０３に関するチームデータリストの内容を更新する（ステップＳ５５）。なお、ステップＳ５４の判断結果が“ＮＯ”であったならば、権限確認機能３５は改竄や不正行為があったものとして処理を中止し、上述したステップＳ５５における保存処理は実施しない。

【００４８】

以上のようにして、サーバＳＶ側に保管されているチームデータリストに基づ

いて、メンバＸが間違いなくルートチームのチームマスタＡによる管理体系の中で正当にチーム１０３のチームマスタとして任命されていることが検証できる（図５のステップＳ２１）。

【００４９】

〈サブチームのチームマスタの変更〉

次に、サブチームのチームマスタを変更するための処理手順について図９を参照して説明する。ここではルートたるチーム１０１にサブオーソリティとして登録されているメンバＢが、サブチームであるチーム１０３のチームマスタをメンバＸからメンバＺへ変更する場合を例に挙げることとする。これは人事一課長が異動になったために、人事部長の代わりに部長代理が課長を変更する場合などに相当する。まず、チームデータリスト管理装置３０はサブチーム１０３に関わるチームデータリストの変更要求をチームデータリスト保管装置３１に送出する（ステップＳ６１）。これにより、チームデータリスト保管装置３１は図５のステップＳ１２と同様にチーム１０１とその配下のサブチームに関するチームデータリストをチームデータリスト管理装置３０側に転送する（ステップＳ６２）。

【００５０】

チームデータリスト管理装置３０では、リスト正当性確認機能３７が図７で説明した処理手順に従って転送されてきたチームデータリストの正当性の検証を行い（ステップＳ６３）、その正当性が検証できた場合に転送されてきたチームデータリストをＡＵＤ・ＡＵＬ変更機能３８に引き渡す。ＡＵＤ・ＡＵＬ変更機能３８は、メンバＢからの指示内容に従って、引き渡されたチームデータリストのうちオーソリティデータ１０３ｄについてチームマスタをメンバＸからメンバＺに変更して、この変更されたオーソリティデータと引き渡されたオーソリティリストとを電子署名機能３９に送る。電子署名機能３９は送られたチームデータリストに対してそれぞれ前述した秘密鍵ファイル等からメンバＢに関する秘密鍵を取得してデジタル署名を施し、それによってオーソリティデータ１０３ｄｂ及びオーソリティリスト１０３ｕｂを作成（ステップＳ６４）したのち、これらチームデータリストをチームデータリスト保管装置３１に転送して保存要求を行う（ステップＳ６５）。

【００５１】

チームデータリスト保管装置３１では、権限確認機能３５が転送されてきたチームデータリストを基に図８に示した手順に従った権限確認を行って、その正当性が確認された場合に、転送されてきたチームデータリストを記憶装置３２に保存する。ここで、サブチーム作成時（図５のステップＳ２１）と相違する点は、チームマスタ変更処理においてはオーソリティリスト１０３ｕｂの署名者であるメンバＢとオーソリティデータ１０３ｄｂで指名されているチームマスタたるメンバＺが異なっていることである（ステップＳ５４の判断結果が“ＮＯ”となるケース）。そこでこの場合、権限確認機能３５はオーソリティリスト１０３ｕｂの署名者が親チームに登録された管理者たるチームマスタＡ，サブオーソリティＢ，サブオーソリティＣの何れかに一致していれば、正当な権限を持つ者による署名であると判断する。そして以上のようにして、サーバＳＶ側にはチーム１０３に関わるチームデータリストとして作成時間の異なる２組のオーソリティリスト及びオーソリティデータ，即ちチームマスタ変更前後の各チームデータリストが保存される。その後、チームデータリスト保管装置３１は、チーム１０３の新たなチームマスタであるメンバＺの署名をオーソリティリスト１０３ｕｂに付与するために、オーソリティデータ１０３ｄｂ及びオーソリティリスト１０３ｕｂをチームデータリスト管理装置３０に転送する（ステップＳ６６）。

【００５２】

チームデータリスト管理装置３０では、リスト正当性確認機能３７が図７の処理手順に従って、転送されてくるチームデータリストの正当性を検証したのち、これをＡＵＤ・ＡＵＬ変更機能３８を介して電子署名機能３９に渡す。電子署名機能３９は、前述した秘密鍵ファイル等からメンバＺに関する秘密鍵を取得し、これを基にオーソリティリスト１０３ｕｂに対してメンバＺのデジタル署名を行ってオーソリティリスト１０３ｕｃを作成する（ステップＳ６７）。次いで、電子署名機能３９は作成されたオーソリティリスト１０３ｕｃをオーソリティデータ１０３ｄｂとともにチームデータリスト保管装置３１に転送する（ステップＳ６８）。チームデータリスト保管装置３１では、権限確認機能３５が転送されてきたチームデータリストを基に図８の処理手順に従って権限確認を行い、その正

当性が確認された場合に転送されてきたチームデータリストを記憶装置３２に保存して、チーム１０３に関わるチームデータリストの更新処理を行う。以上によって、チームマスタが正常な手順を踏んで変更されたことになる。

【００５３】

〈サブオーソリティの変更〉

次に、サブオーソリティを変更するための処理手順について図１０を参照して説明する。ここでは、ルートであるチーム１０１のチームマスタＡが、このチーム１０１でサブオーソリティとして登録されているメンバＢの作成権限を剥奪する場合を例に挙げて説明する。これは、部長代理が異動になるなどして、人事部長がこの部長代理を人事部から除外する場合などに相当する。なお、同図では図９に示したチームマスタ変更によってサブオーソリティＢが作成者となっているチーム１０３を前提としている。また、同図では、サブオーソリティＢの作成権限が削除されるのに伴ってチーム１０３を削除してしまう場合と、チーム１０３を継続させる場合の２つのケースを併せて図示してある。したがって、メンバＡがチームデータリスト管理装置３０に対して要求を指示する場合にはチーム１０３を存続させるかのか否かも併せて指示するようにしている。

【００５４】

まず、チームデータリスト管理装置３０はチーム１０１に登録されているサブオーソリティＢに対する変更要求（削除要求）をチームデータリスト保管装置３１に対して送出する（ステップＳ７１）。これにより、チームデータリスト保管装置３１はチーム１０１の配下にあるサブチームのオーソリティデータを参照して、それらサブチームの中からサブチームＢが作成者となっているチーム１０３を検索したのち、チーム１０１とチーム１０３に関するチームデータリストをチームデータリスト管理装置３０側に転送する（ステップＳ７２）。チームデータリスト管理装置３０では、リスト正当性確認機能３７が図７で説明した処理手順に従って、転送されてきたチームデータリストの正当性の検証を行い、その正当性が検証できた場合に転送されてきたチームデータリストをＡＵＤ・ＡＵＬ変更機能３８に引き渡す。

【００５５】

ＡＵＤ・ＡＵＬ変更機能３８はメンバＡからの指示内容に基づいて、引き渡されたチームデータリストのうち、オーソリティリスト１０１ｕに記述されているサブオーソリティの中からメンバＢを削除したオーソリティリスト１０１ｕｂを作成する（ステップＳ７３）。これに加えて、ＡＵＤ・ＡＵＬ変更機能３８はオーソリティデータ１０３ｄｂに付与されているメンバＢの署名を削除してオーソリティデータ１０３ｄｃを作成する（ステップＳ７４）。この後、ＡＵＤ・ＡＵＬ変更機能３８はオーソリティデータ１０３ｄｃとオーソリティリスト１０３ｕｃを電子署名機能３９に送出する。

【００５６】

電子署名機能３９はメンバＡからの指示内容に従って以下の２通りの処理の何れかを行う。第１に、チーム１０３を継続させる要求が来ているのであれば、電子署名機能３９はチーム１０３の存在をメンバＡが承認したものと見なし、前述した秘密鍵ファイル等からメンバＡに関する秘密鍵を取得し、これを基にオーソリティデータ１０３ｄｃにメンバＡの署名を添付してオーソリティデータ１０３ｄｄを作成する（ステップＳ７５）。次いで、電子署名機能３９はオーソリティデータ１０１ｄ，１０３ｄｄ及びオーソリティリスト１０１ｕｂ，１０３ｕｃをチームデータリスト保管装置３１に転送してこれらチームデータリストの保存要求を行う（ステップＳ７６）。チームデータリスト保管装置３１では、権限確認機能３５が転送されてきたチームデータリストを基に図８に示した手順に従った権限確認を行って、その正当性が確認された場合に、転送されたチームデータリストで記憶装置３２の内容を更新する（ステップＳ７７）。

【００５７】

第２に、チーム１０３を消去する旨の要求が来ているのであれば、電子署名機能３９はチーム１０１に関するチームデータリスト，すなわちオーソリティデータ１０１ｄ及びオーソリティリスト１０１ｕｂをチームデータリスト保管装置３１へ転送するとともに、チーム１０３を無効にする旨の命令をチームデータリスト保管装置３１に送出する（ステップＳ７８）。チームデータリスト保管装置３１では、権限確認機能３５が記憶装置３２に保存されているオーソリティリスト１０１ｕと送られてきたオーソリティリスト１０１ｕｂを照合することでサブオ

ーソリティＢの削除を認識することができる。これに加えて、権限確認機能３５はオーソリティデータ１０１ｄ及びオーソリティリスト１０１ｕｂの内容から、チームマスタがメンバＡであって且つこれらチームデータリストが何れもこのメンバＡによってデジタル署名されていることが分かる。こうしたことから、権限確認機能３５はチームマスタＡが正当な権限でサブオーソリティＢを削除したものと判断して、オーソリティデータ１０１ｄ及びオーソリティリスト１０１ｕｂの内容で記憶装置３２中のチーム１０１のチームデータリストを更新する。次いで、権限確認機能３５は記憶装置３２上からチーム１０３に関わるオーソリティデータ及びオーソリティリストを削除する（以上、ステップＳ７９）。以上によって、サブオーソリティＢの作成権限がサーバＳＶ上のチームデータリストから削除されたことになる。

【００５８】

〈サブチームの削除〉

次に、サブチームを削除するための処理手順について図１１を参照して説明する。ここでは、ルートであるチーム１０１にサブオーソリティとして登録されているメンバＣが、前述した図５の処理手順で作成したチーム１０３を削除する場合を例に挙げて説明する。これは、人事部の下にある人事一課が廃止されたために、人事部長代理が課の廃止に関わる業務を行う場合などに相当する。ここで、メンバＣは、サブチームであるチーム１０３の親に相当するチーム１０１のサブオーソリティの権限でもってチーム１０３を削除するため、自分が間違いなくメンバＣ本人であることをチームデータリスト保管装置３１に対して証明してやる必要がある。そのため、チームデータリスト管理装置３０は後述するようにチームデータリスト保管装置３１に対してメンバＣの電子署名を通知するようにしている。

【００５９】

さて、まずメンバＣがチームデータリスト管理装置３０に対してチーム１０３の削除指示を行うと、チームデータリスト管理装置３０は電子署名機能３９によってメンバＣの電子署名を作成したのち、チーム１０３をメンバＣの権限で削除する旨の命令とメンバＣの電子署名を組にしてチームデータリスト保管装置３１

へ転送する（ステップＳ８１）。なお、電子署名を添付する以外の方法として、削除命令の転送時に証明する「シェイクハンド」あるいは「チャレンジレスポンス」と呼ばれる方法（詳細は後述）を採用することも考えられるが、ここでは電子署名を用いた方法に沿って説明を行うものとして、最後にシェイクハンドについて説明することとする。

【００６０】

チームデータリスト保管装置３１がチームデータリスト管理装置３０からチーム１０３の削除命令を受け取ると、権限確認機能３５はチーム１０１及びチーム１０３に関するチームデータリストを参照して、チーム１０１に登録されているサブオーソリティＣがチーム１０３の作成者であることを知る。また、権限確認機能３５はオーソリティデータ１０３ｄに記述されたメンバＣの署名と削除命令に添付されているメンバＣの署名を照合して、これらが一致していることことを確認することにより、削除を指示した者が間違いなくメンバＣ本人であることについて確証を持てる。こうして、権限確認機能３５は正当な権限で発行された削除命令であるものと判断して、記憶装置３２上からチーム１０３に関するオーソリティデータ１０３ｄ及びオーソリティリスト１０３ｕを削除する（以上、ステップＳ８２）。以上によって、サブオーソリティＣによるチーム１０３の削除処理が完了したことになる。

【００６１】

ところで、メンバＡはチーム１０１のチームマスタであることから、サブオーソリティＣの代わりにサブチームたるチーム１０３を削除する正当な権限を有している。この場合に、メンバＡがチームデータリスト管理装置３０に対してチーム１０３の削除指示を行うと、チームデータリスト管理装置３０は電子署名機能３９によってメンバＡの電子署名を作成して、チーム１０３をチームマスタＡの権限で削除する旨の命令とメンバＡの電子署名をチームデータリスト保管装置３１へ転送する（ステップＳ８３）。チームデータリスト保管装置３１において、権限確認機能３５はチーム１０１及びチーム１０３に関するチームデータリストを参照することで、チーム１０１に登録されているサブオーソリティＣがチーム１０３の作成者であり、且つ、このサブオーソリティＣは親チーム１０１のチー

ムマスタＡによってサブオーソリティとして指名されたものであることが分かる。また、権限確認機能３５はオーソリティデータ１０１ｄに記載されているメンバＡの署名と削除命令に添付されているメンバＡの署名を照合することで、削除を指示した者が間違いなくメンバＡ本人であることを確認する。こうして、権限確認機能３５は正当な権限で発行された削除命令であるものと判断して、記憶装置３２上からチーム１０３に関するオーソリティデータ１０３ｄ及びオーソリティリスト１０３ｕを削除する（以上、ステップＳ８４）。

【００６２】

以上によって、チームマスタＡによるチーム１０３の削除処理が完了したことになる。なお、上述したメンバ以外にも、例えばチーム１０１にサブオーソリティとして登録されているメンバＢがサブチームであるチーム１０３を削除することも可能である。

【００６３】

最後に、図１２を参照しつつ、上述したシェイクハンドないしチャレンジレスポンスの処理手順の詳細を説明する。まず、クライアントＣＬはサーバＳＶにアクセスする際にユーザ（図１１の場合で言えばメンバＣまたはメンバＡ）のユーザ名およびユーザ公開鍵をサーバＳＶに送付する（ステップＳ１０１）。サーバＳＶは乱数を発生させて内部に記憶するとともにこの乱数をユーザ公開鍵で暗号化（ステップＳ１０２）し、暗号化されたデータを「チャレンジデータ」としてクライアントＣＬに送信する（ステップＳ１０３）。クライアントＣＬはサーバＳＶから送られたチャレンジデータをユーザ公開鍵に対応した秘密鍵で復号化（ステップＳ１０４）し、得られた復号化データを「チャレンジレスポンス」としてサーバＳＶに返送する（ステップＳ１０５）。サーバＳＶはクライアントＣＬから送られたチャレンジレスポンスとステップＳ１０２で発生させた乱数とを比較して通信相手を確認する。すなわち、両者が一致すればステップＳ１０１で送付されたユーザ公開鍵に対応する秘密鍵を知っている者が通信相手であることを確認（認証成功）することができる。これに対し、両者が不一致であれば通信相手が正当な権限を持った者でない可能性のある（認証失敗）ことがわかる（以上、ステップＳ１０６）。この後、サーバＳＶはステップＳ１０６で得られた確認

結果（認証成功または認証失敗）をクライアントＣＬに通知する（ステップＳ１０７）。以上のようにすることで、電子署名を添付した場合と同じく、メンバＣやメンバＡが本人であることをサーバＳＶ側で確かめることができる。

【００６４】

なお、クライアントＣＬからサーバＳＶへユーザ公開鍵を送る代わりに「ユーザ公開鍵番号」を送るようにしても良い。ここで言うユーザ公開鍵番号はユーザ本人を識別・認証するための情報であって、各ユーザ公開鍵に予め付与されているシリアル番号のことである。さらに詳しく説明すると、ユーザ公開鍵番号はユーザ公開鍵を一意に識別するための各ユーザ公開鍵に対応した情報であって、例えば、上述した認証局から発行された証明書に含まれている当該証明書のシリアル番号である。また、ユーザ本人を識別・認証するための情報としては、いま述べたユーザ公開鍵番号以外にも、実際に鍵作成者本人を識別するＩＤや名前などの様々な情報を利用することができる。

【００６５】

〔第２実施形態〕

図１３は本実施形態によるチームの階層化について示したものであって、チーム内のメンバの利用できるアプリケーションがチーム毎に異なる形態を実現したものである。同図では、図４に示したチームのうちチーム１０１～１０３に対応するものだけを示してある。オーソリティリスト及びオーソリティデータに関しては図４に示したものと同じであるが、このほか、各チームにはメンバリストの代わりにメンバリストの内容を包含するアプリケーションリスト１０１ａ，１０２ａ，１０３ａが設けられている。すなわち、これらアプリケーションリストには、各チームに属するメンバの利用可能なシステムのほか、そのチームに属するメンバの一覧が記載されている。アプリケーションについては例えばチーム１０１のアプリケーションリスト１０１ａには人事管理システム，経理システム，スケジュール，ファイル共有システムが登録されている。また、メンバ一覧については図４のメンバリストに記載されているものと同じである。

【００６６】

この第２実施形態では、第１実施形態と同様にチームの生成に関しては親チー

ムの干渉を受けるものの、アプリケーションリストは各チームのチームマスタがそれぞれ署名するので、チーム内の管理は親チームからの干渉を受けずに行うことができる。つまり、チーム内で利用可能なアプリケーションをどのメンバで共同利用するかといったことは、チームマスタが親チームの管理者から独立して行うことができる。例えば、チーム１０１のサブチームであるチーム１０２では、アプリケーションリスト１０２ａの署名はチーム１０２のチームマスタであるメンバＹが署名しており、チーム１０１の管理者であるチームマスタＡやサブオーソリティＢ，Ｃの干渉を受けなくて済む。

【００６７】

〔第３実施形態〕

本実施形態では、サブチームを管理するという観点から見たメンバ，サブオーソリティ，チームマスタという上述の権限分担に加えて、情報を共有してゆくためのチーム内での管理権限分担として各チームに属する者をメンバ，サブマスタ，チームマスタの３種類に分類している。このうち、サブマスタはチームマスタによって指名されたチーム内の管理者であって、チームマスタやサブマスタを変更することは許されていないが、一般のメンバについて追加，削除，変更を行うことのできる者である。一方、チームマスタはサブマスタ又はメンバの変更を行えるほか、自身のチームマスタでさえ変更することのできる者である。他方、サブマスタ及びチームマスタ以外の一般のメンバはメンバに提供される情報や機能を共有する者であって、チームデータリストの内容に変更を加える等の権限はいっさい与えられていない。なお、サブマスタやチームマスタも特別な権限が与えられてはいるが、チーム内のメンバであることに変わりはなく、その意味でサブマスタ又はチームマスタをメンバと呼ぶことがある。

【００６８】

図１４は本実施形態におけるチームの階層化について示したものである。同図では、図４に示した第１実施形態の各チームに対してさらにチームマスタリストを加えてある。こうすることで、チーム毎に情報共有を管理するとともに、各チーム内の情報共有のメンバの管理を複数の管理者が行えるようにしている。図１４において、チームマスタリスト１０１ｔ～１０４ｔは各チームに登録されてい

るチームマスタ及びサブマスタの一覧とチームマスタの署名が記載されている。もっとも、これ以外にもチームマスタリストには、チームマスタ又はサブマスタの識別情報，公開鍵，公開鍵ＩＤ，チームＩＤ，チームマスタリストの作成時間を示すタイムスタンプなどが含まれている。このほか、チームマスタリスト３４には、チームに関する情報としてチームのメンバ数，チームの作成された時間，チーム内の各メンバが利用することのできる各種機能などの情報（例えば、上述したアプリケーションリスト）も含まれており、これらを用いることで各チームに関する情報リソースの管理を同時に行うことができる。

【００６９】

チームマスタリストの署名は、各チームのチームマスタがチーム作成時に署名し、以後はずっとチームマスタの署名になっている。これに対し、メンバリストについては各チーム内のチームマスタの他に、サブマスタがこれを管理する権限を付与されているため、チームマスタ以外にサブマスタの署名が為されている場合もある。例えば、メンバリスト１０１ｍａに関してはチーム１０１のサブマスタとして登録されているメンバＢの署名がなされている。一方、チーム１０２のように、チームマスタリスト１０２ｔにサブマスタが登録されていない場合にはメンバリスト１０２ｍａはチームマスタであるメンバＢが署名することになる。

【００７０】

この図１４ではサブチームの管理権限，メンバの管理権限をそれぞれオーソリティリスト／オーソリティデータ，チームマスタリストに分割しているため、各チーム内でサブオーソリティとサブマスタに異なる者を割り当てることができる。例えば、チーム１０３ではメンバW及びメンバＶがサブオーソリティであり、メンバＹ及びメンバＺがサブマスタであるため、サブチームの管理とメンバ管理を異なる者が担当して負荷分散を図ることもできる。もっとも、実際にはサブオーソリティとサブマスタを同じメンバにしてしまって良い。その場合はオーソリティリストとメンバリストを統合して一つのリストにしてしまうことが可能となる。

【００７１】

〔第４実施形態〕

上述した各実施形態では、チームデータリストを使用する都度、チームマスタが間違いなく自分のチームマスタであるかどうかをユーザがクライアントＣＬ側で確認する必要がある。例えば、チームデータリスト管理装置３０を構成するコンピュータのディスプレイ上に、“このリストは以下のメンバが管理者となって正常に管理されています。名前：メンバＡ。組織：三菱マテリアル株式会社。作業を続行する場合はＯＫボタンをマウスでクリックして下さい”などといったメッセージが表示される。このように、ユーザは当該メッセージを目視で確認する必要が生じてくるため、ユーザに対して煩わしい印象を与える可能性がないとは言えない。こうした点を改善するには以下の機能をリスト正当性確認機能３７と連携する新たな機能として追加し、あるいは、リスト正当性確認機能３７の一機能として組み込むようにすることで解決される。

【００７２】

すなわち、ルートチーム１０１におけるチームマスタの公開鍵をチーム毎に予めクライアントＣＬ側の例えば公開鍵データベース４１（図１参照）に登録しておき、公開鍵管理機能４０が公開鍵データベース４１からチーム１０１のチームマスタに関する公開鍵を取得してこれをリスト正当性確認機能３７に通知する。もしくは、公開鍵データベース４１には公開鍵に関する情報として公開鍵を識別するためのシリアル番号等を登録しておき、公開鍵管理機能４０がこのシリアル番号を公開鍵データベース４１から取得したのち、これをもとにチームデータリスト管理装置３０の外部（例えばインターネット上）に登録されている公開鍵を別途取得してリスト正当性確認機能３７に渡すように構成しても良い。

【００７３】

一方、リスト正当性確認機能３７は、コンピュータのディスプレイ上に上述したようなメッセージを出す代わりに、公開鍵管理機能４０から通知されるチーム１０１のチームマスタの公開鍵に基づいて、チームデータリスト保管装置３１から転送されてくるオーソリティデータ１０１ｄに含まれているチームマスタのデジタル署名を確認するようにして、当該署名が登録されているチームマスタのものかどうかを判断する。こうすることで、ユーザがディスプレイ上の表示をもとに目視で確認することなく、ルートチーム１０１のチームマスタの正当性を検証

できるようになる。

なお、チームマスタを確認するための情報としては公開鍵以外にも様々な情報を利用できるのはもちろんである。

【００７４】

以上の通り、チームを階層化するためのチームデータリストを管理するチームデータリスト管理プログラムを記録した記録媒体において、チームデータリスト管理プログラムは、（１）所定の要求先に前記チームデータリストの操作要求を行う処理と、（２）前記操作要求に応じて、操作対象のチームからルートチームに至る各チームについて、自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータと、自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストを有するチームデータリストを前記要求先から取得する処理と、（３）前記識別子を用いて取得された各チームを前記ルートチームまで辿りながら各チームについて、前記チームデータリストの電子署名が改竄されていないこと及び前記管理者情報を用いて権限を持つ者による署名であることを確認したのち、ユーザによる前記ルートチームのチームマスタの承認を確認する正当性確認処理と、（４）該正当性確認処理によって正当性が確認された前記チームデータリストに対して前記操作要求に応じた変更を加える変更処理と、（５）前記操作要求を行った指示者の電子署名を作成して、前記変更処理によって変更されたチームデータリストに該電子署名を添付して前記要求先に送出する処理とをコンピュータに実行させる。

【００７５】

また、上述のチームデータリスト管理プログラムにおいて、前記正当性確認処理は、前記チームマスタにより自チーム内のメンバから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報を前記管理者情報として用いるものであっても良い。

また、上述のチームデータリスト管理プログラムは、前記ルートチームのチー

ムマスタの本人識別を行うための識別情報を所定の場所から取得して予め登録しておく処理と、前記要求先から前記ルートチームのオーソリティデータが送られてくる度に、予め登録されている前記識別情報を用いて、該オーソリティデータの電子署名が前記チームマスタの電子署名であることを確認する処理とをさらにコンピュータに実行させるものであっても良い。

【００７６】

一方、チームを階層化するためのチームデータリストを保管するチームデータリスト保管プログラムを記録した記録媒体において、チームデータリスト保管プログラムは、（１）自チームの親チームを表す識別子及び前記親チームの管理者の電子署名が含まれたオーソリティデータをチーム毎に予め記憶しておく処理と、（２）自チームの管理下にあるサブチームの管理権限者に関する管理者情報及び自チームの管理者であるチームマスタ又は前記親チームの管理者の電子署名が含まれたオーソリティリストをチーム毎に予め記憶しておく処理と、（３）所定の要求元から前記オーソリティデータ及び前記オーソリティリストが少なくとも含まれたチームデータリストに対する操作要求があったときに、該操作要求の指示者が要求権限を持つことを前記管理者情報を用いて確認するとともに、該操作要求が参照要求或いは削除要求である場合は、要求されたチームデータリストを前記要求元へ返送し或いは削除し、該操作要求が更新要求である場合は、前記要求元から送られるチームデータリストの電子署名が権限を持つ者による署名であることを前記管理者情報を用いて確認したのち、前記送られたチームデータリストで記憶されている前記オーソリティデータ及び記憶されている前記オーソリティリストを更新する権限確認処理とをコンピュータに実行させる。

また、上述のチームデータリスト保管プログラムにおいて、前記権限確認処理は、前記チームマスタにより自チーム内のメンバから指名された者であって前記サブチームの管理権限を有する一人以上のサブオーソリティと、前記サブオーソリティの持つ権限に加えて前記サブオーソリティに対する管理権限を有する前記チームマスタとに関する情報を前記管理者情報として用いるものであって良い。

【００７７】

【発明の効果】

以上説明したように、本発明では、オーソリティリストとオーソリティデータの含まれたチームデータリストを用いることで各チームの下にサブチームを作成することができ、階層化されたチームを構築することができる。また、ユーザはルートチームのチームマスタの署名を確認するだけで、操作対象のチームからルートチームに至る各チームについてチームデータリストの正当性を確認することができる。さらに、親チームの管理者の指示によって誰もがサブチーム内の管理を行うチームマスタになることができる。

また、本発明では、チームデータリストを親チームの管理下にあるオーソリティデータと自チームの管理に関わるオーソリティリストに分割しており、各チームのチームマスタが親チームの干渉を受けることなく情報共有メンバの管理といった自チーム内の管理を行うことができ、一方で、親チームの管理者はサブチーム内部の管理に関与する必要がなくなる。

また、本発明では、チームデータリストに対して正当な権限を持つ者による電子署名を含ませているため、改竄等の不正な行為を検出することが可能となる。

また、本発明では、チームデータリストの操作要求がなされた場合に、これら要求の指示者が権限を持つ者かどうかの権限確認を実施しているので、サーバの管理者，チーム内の一般のメンバ，クラッカ等の権限を持たない者による不正な行為を未然に防止することができる。

また、本発明では、特に選定されたチームマスタと一人以上のサブオーソリティに対してサブチームの管理権限を与えており、チームマスタ自身がサブオーソリティを選任できるほか、複数の管理者がサブチームを管理できるため管理負担が分散される。

また、本発明では、公開鍵などのルートチームのチームマスタ本人を識別・認証するための識別情報を予め登録しておき、この識別情報をもとに、ルートチームのチームマスタを確認しているため、チームデータリストを操作する度にユーザ自身が目視で確認するなどの煩わしい作業が必要なくなり、ルートチームのチームマスタを自動的に承認することが可能となる。

【図面の簡単な説明】

【図１】　本発明の第１実施形態によるチームデータリスト管理装置及びチ

ームデータリスト保管装置を有するシステムの構成を示したブロック図である。

【図２】　同実施形態において、チームデータリスト保管装置が設置されたサーバ側に記憶されるチームデータリストの構造を示した説明図であって、（ａ）はオーソリティデータの構造，（ｂ）はオーソリティリストの構造，（ｃ）はオーソリティデータの簡略化表記，（ｄ）はオーソリティリストの簡略化表記である。

【図３】　同実施形態におけるチームの階層の一例を示した説明図である。

【図４】　図３に示すチーム階層の各チームについてチームデータリストの具体的な値を記入した説明図である。

【図５】　同実施形態においてサブチームを作成するための処理手順を示した説明図である。

【図６】　図５の処理過程でサブチーム作成要求時に行われるサーバ側の権限確認機能についてその処理手順を示した説明図である。

【図７】　図５の処理過程で実施されるクライアント側のリスト正当性検証に関わる処理手順を示した説明図である。

【図８】　図５の処理過程において、クライアント側で新規に作成したチームデータリストをサーバ側で権限確認を行う際の処理手順を示す説明図である。

【図９】　同実施形態において、サブチームのチームマスタを変更するための処理手順を示した説明図である。

【図１０】　同実施形態において、サブオーソリティの作成権限を変更（削除）するための処理手順を示した説明図である。

【図１１】　同実施形態において、サブチームを削除するための処理手順を示した説明図である。

【図１２】　クライアント側に居るユーザの権限確認を行う際にサーバが用いるシェイクハンドないしチャレンジレスポンスと呼ばれる手法の手順を示した説明図である。

【図１３】　本発明の第２実施形態におけるチームの階層の一例を示した説明図である。

【図１４】　本発明の第３実施形態におけるチームの階層の一例を示した説

明図である。

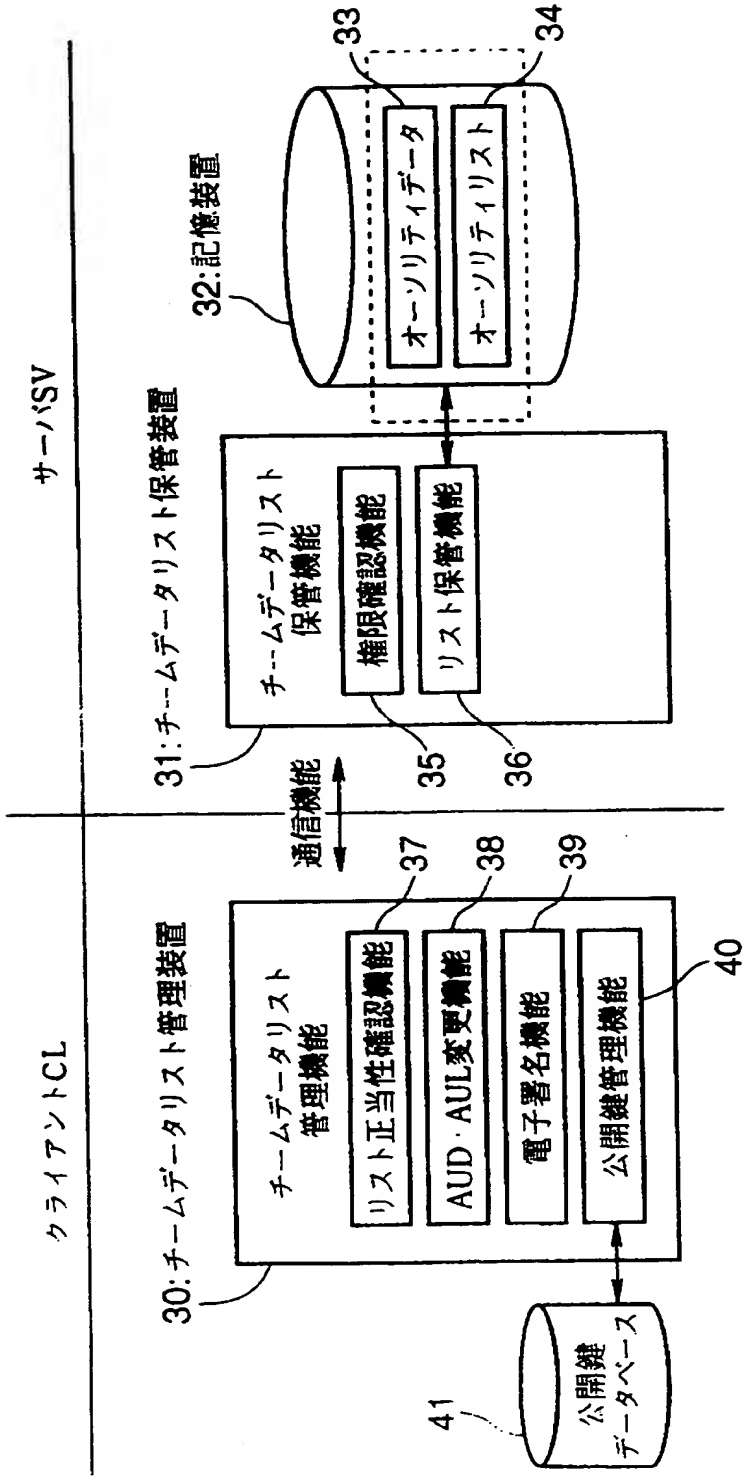
【図１５】　アクセス制御リストを利用して情報共有を行う従来のシステムの構成を示したブロック図である。

【符号の説明】

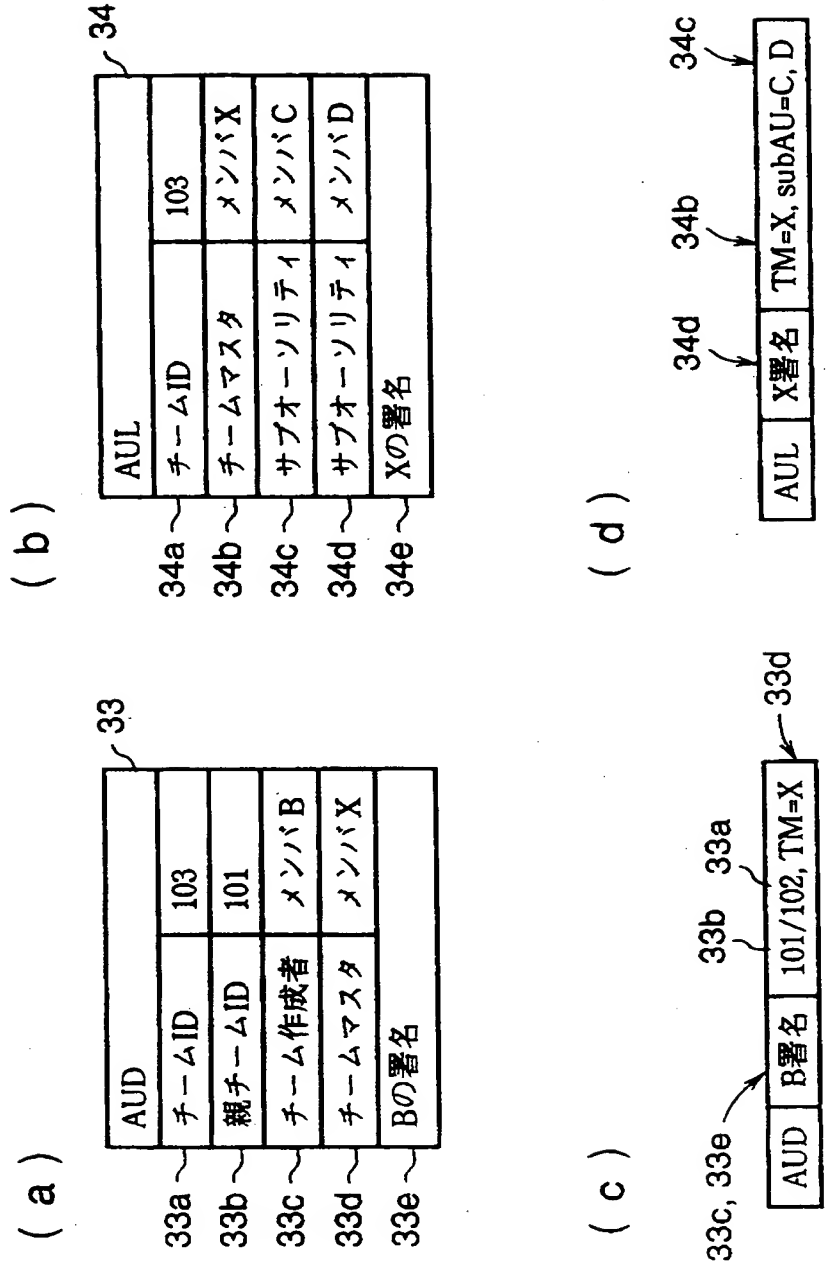
３０…チームデータリスト管理装置、３１…チームデータリスト保管装置、３２…記憶装置、３３…オーソリティデータ、３４…オーソリティリスト、３５…権限確認機能、３６…リスト保管機能、３７…リスト正当性確認機能、３８…ＡＵＤ・ＡＵＬ変更機能、３９…電子署名機能、４０…公開鍵管理機能、４１…公開鍵データベース、ＣＬ…クライアント、ＳＶ…サーバ

【書類名】　図面

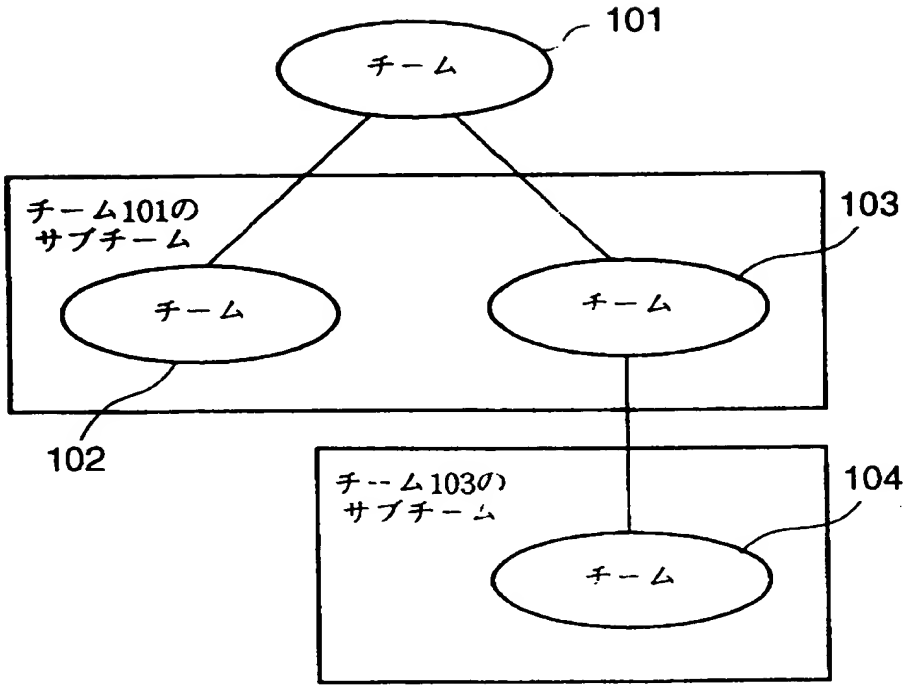
【図１】


サーバSV
クライアントCL
32:記憶装置
33
34
オーソリティデータ
オーソリティリスト
31:チームデータリスト保管装置
チームデータリスト
保管機能
権限確認機能
リスト保管機能
35
36
通信機能
30:チームデータリスト管理装置
チームデータリスト
管理機能
リスト正当性確認機能
AUD・AUL変更機能
電子署名機能
公開鍵管理機能
37
38
39
40
41
公開鍵
データベース

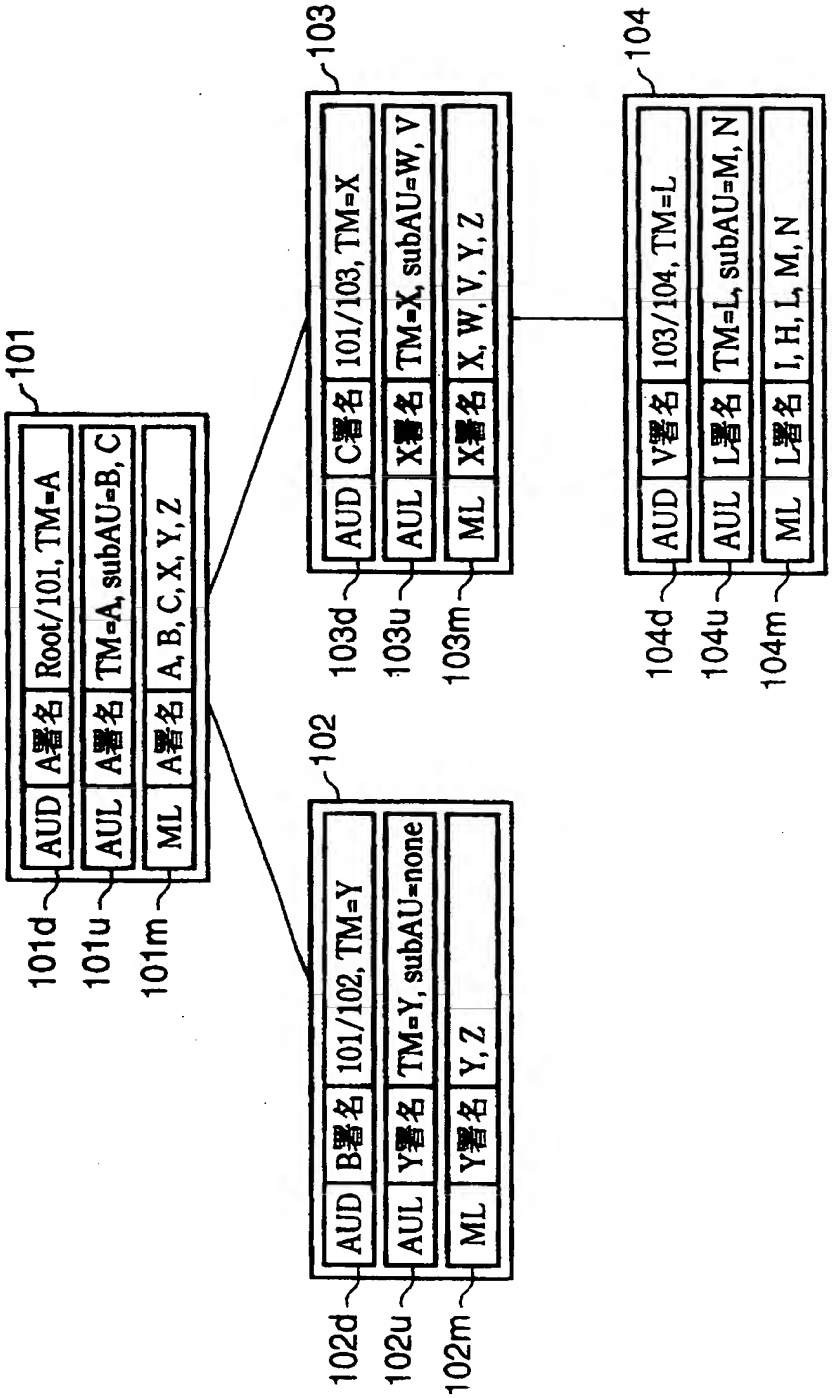
【図２】


(a)
33
AUD
チームID
103
親チームID
101
チーム作成者
メンバB
チームマスタ
メンバX
Bの署名
33a
33b
33c
33d
33e
(b)
34
AUL
チームID
103
チームマスタ
メンバX
サブオーソリティ
メンバC
サブオーソリティ
メンバD
Xの署名
34a
34b
34c
34d
34e
(c)
AUD
B署名
101/102, TM=X
33c, 33e
33b
33a
33d
(d)
AUL
X署名
TM=X, subAU=C, D
34d
34b
34c

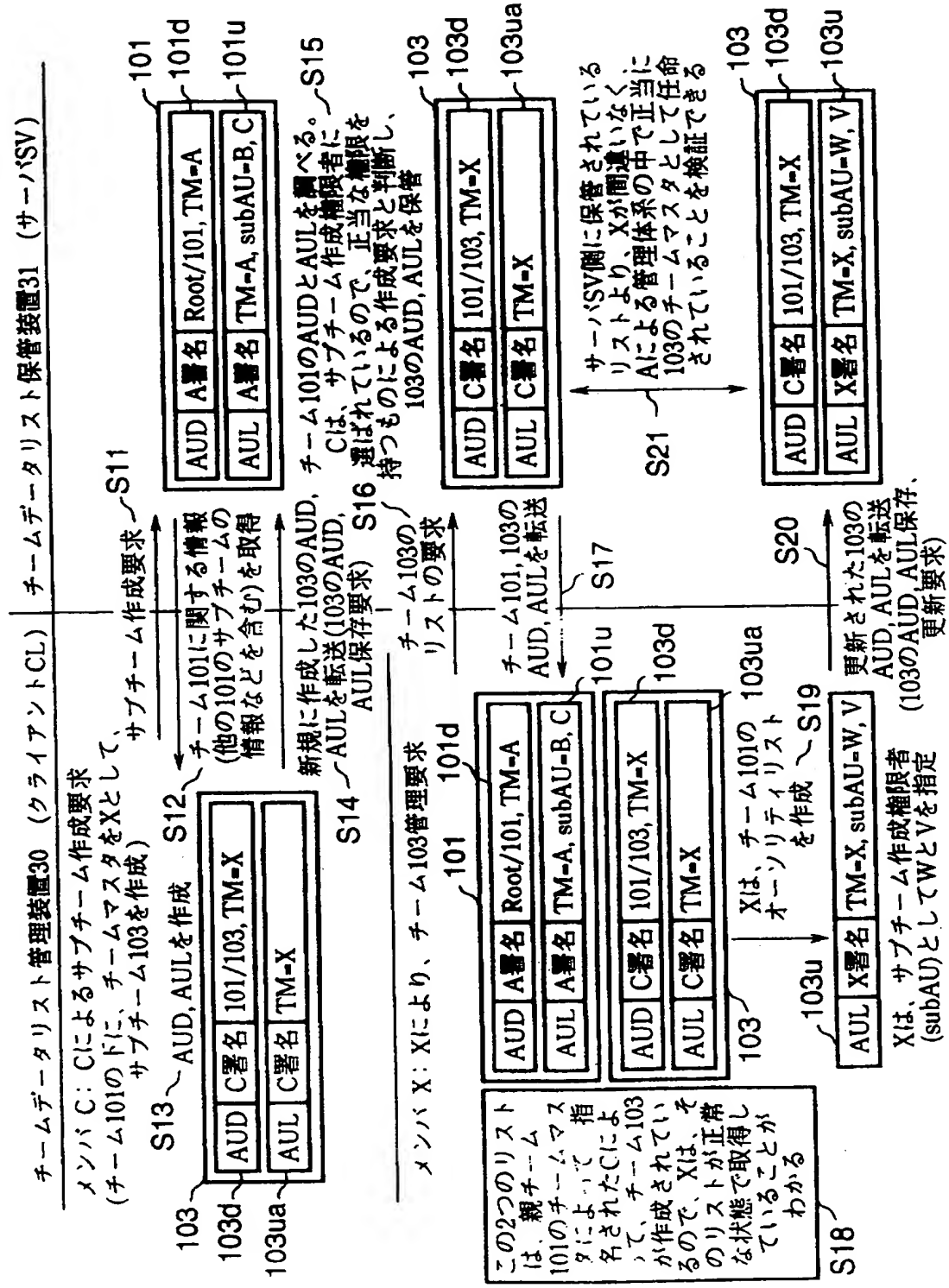
【図３】



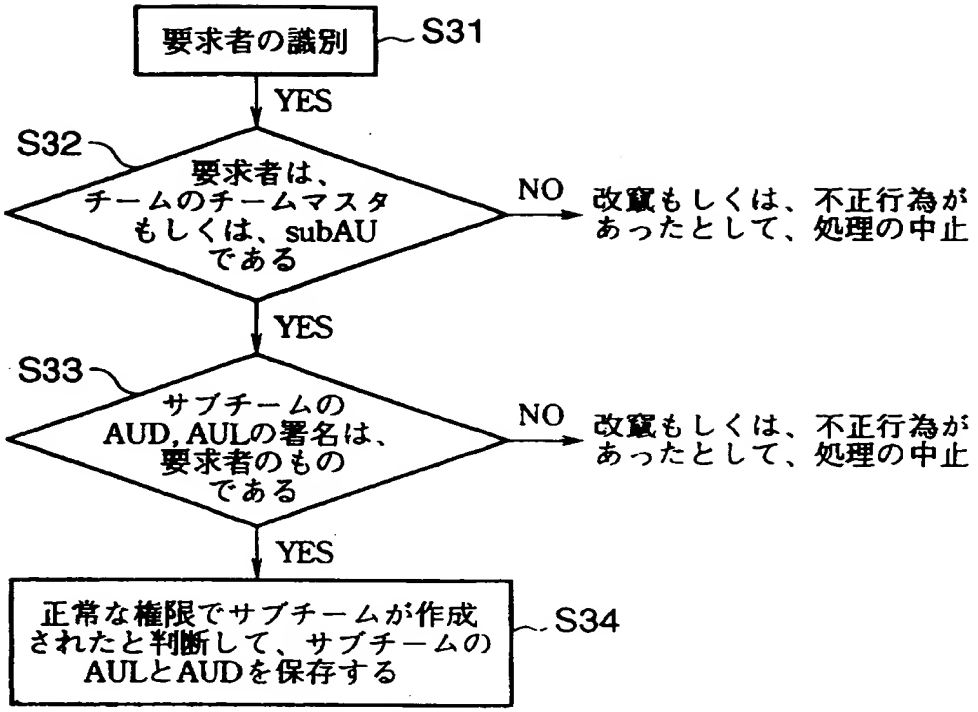
【図４】


101
AUD
A署名
Root/101, TM=A
AUL
A署名
TM=A, subAU=B, C
ML
A署名
A, B, C, X, Y, Z
101d
101u
101m
103
AUD
C署名
101/103, TM=X
AUL
X署名
TM=X, subAU=W, V
ML
X署名
X, W, V, Y, Z
103d
103u
103m
104
AUD
V署名
103/104, TM=L
AUL
L署名
TM=L, subAU=M, N
ML
L署名
I, H, L, M, N
104d
104u
104m
102
AUD
B署名
101/102, TM=Y
AUL
Y署名
TM=Y, subAU=none
ML
Y署名
Y, Z
102d
102u
102m

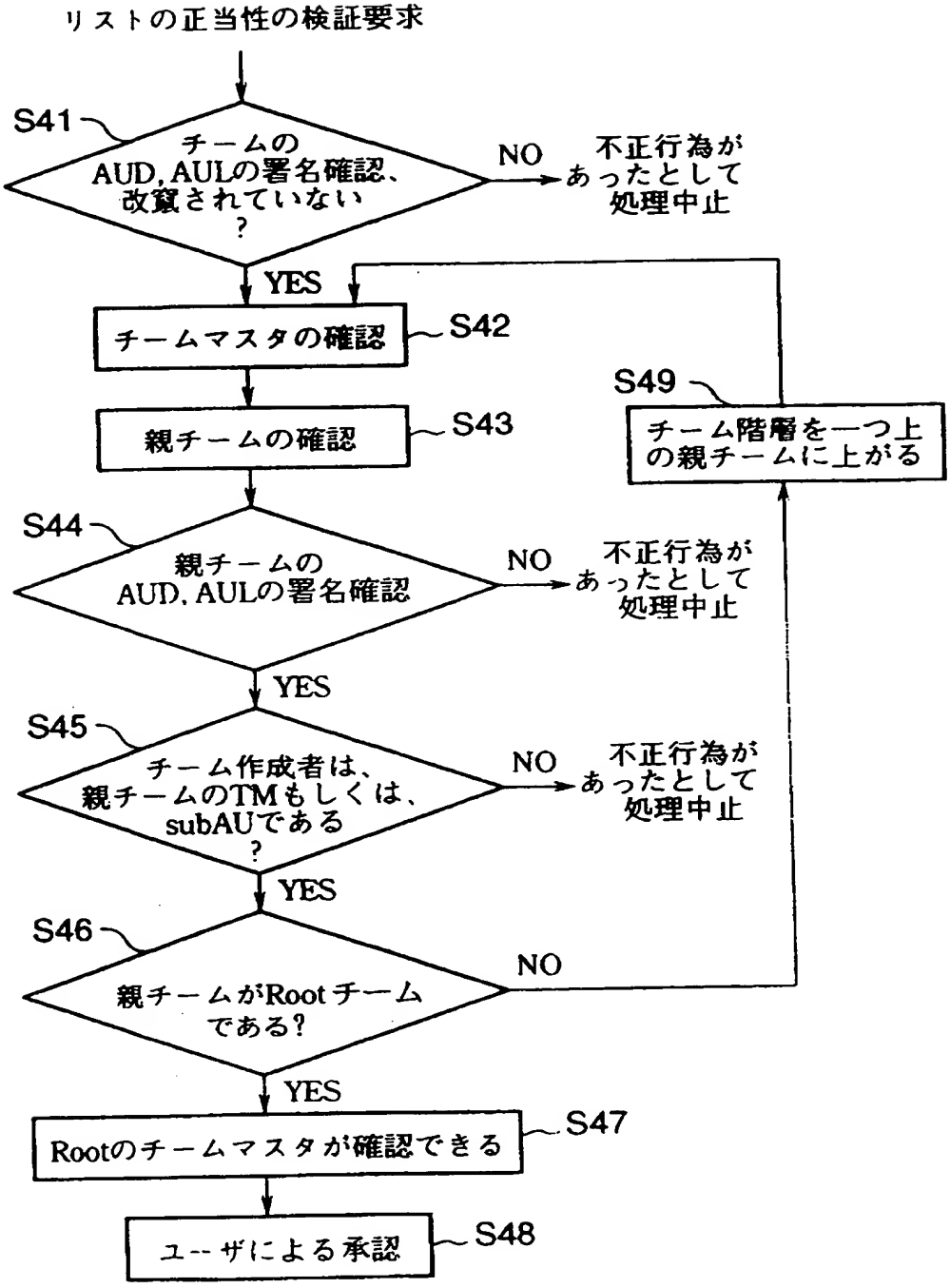
【図５】


チームデータリスト管理装置30 (クライアントCL)
チームデータリスト保管装置31 (サーバSV)
メンバC: Cによるサブチーム作成要求
(チーム101の下に、チームマスタをXとして、サブチーム103を作成)
サブチーム作成要求
S11
S12
チーム101に関する情報
(他の101のサブチームの情報などを含む)を取得
S13
AUD, AULを作成
103
103d
103ua
AUD C署名 101/103, TM-X
AUL C署名 TM-X
101
101d
101u
AUD A署名 Root/101, TM-A
AUL A署名 TM-A, subAU-B, C
新規に作成した103のAUD, AULを転送(103のAUD, AUL保存要求)
S14
チーム101のAUDとAULを調べる。
S15
Cは、サブチーム作成権限者に選ばれているので、正当な権限を持つものによる作成要求と判断し、103のAUD, AULを保管
S16
チーム103のリストの要求
103
103d
103ua
AUD C署名 101/103, TM-X
AUL C署名 TM-X
メンバX: Xにより、チーム103管理要求
101
101d
AUD A署名 Root/101, TM-A
AUL A署名 TM-A, subAU-B, C
チーム101, 103のAUD, AULを転送
S17
サーバSV側に保管されているリストより、Xが間違いなく、Aによる管理体系の中で正当に103のチームマスタとして任命されていることを検証できる
S21
103
103d
103u
AUD C署名 101/103, TM-X
AUL X署名 TM-X, subAU-W, V
AUD C署名 101/103, TM-X
AUL C署名 TM-X
103
Xは、チーム101のオーソリティリストを作成
S19
103u
AUL X署名 TM-X, subAU-W, V
S20
更新された103のAUD, AULを転送(103のAUD, AUL保存、更新要求)
Xは、サブチーム作成権限者(subAU)としてWとVを指定
この2つのリストは、親チーム101のチームマスタによって指名されたCによって、チーム103が作成されているので、Xは、そのリストが正常な状態で取得していることがわかる
S18

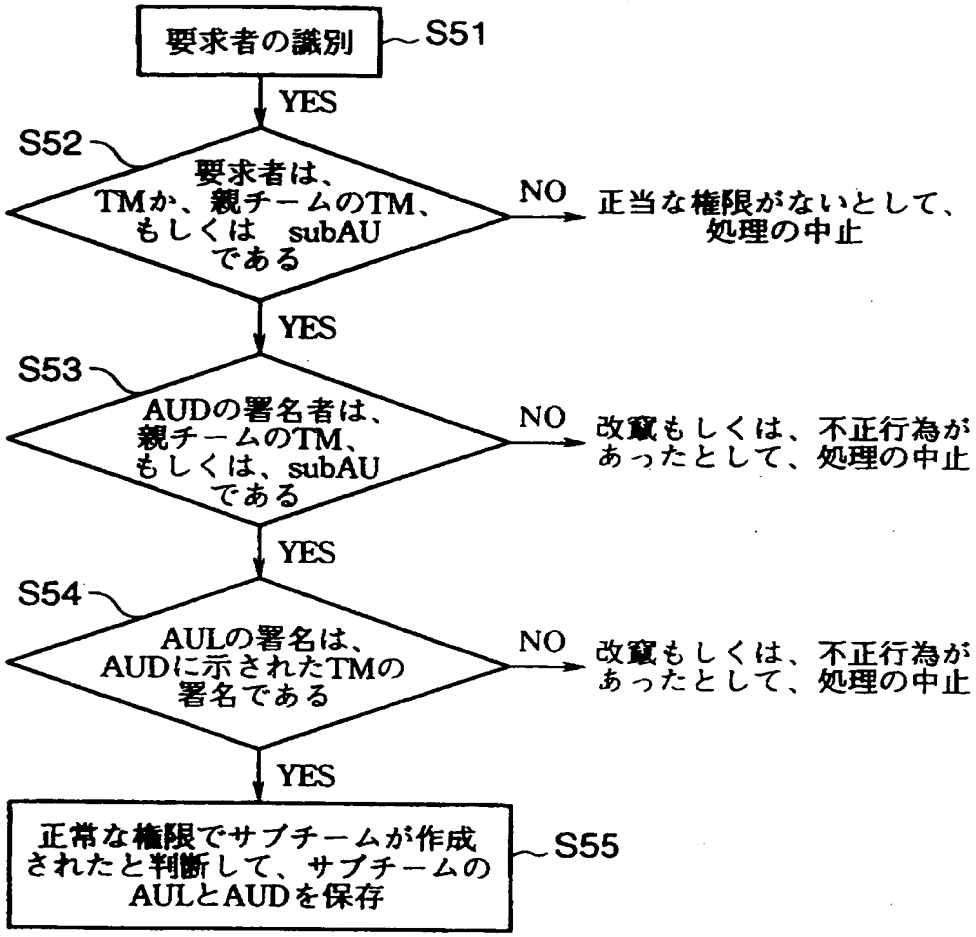
【図６】


要求者の識別
S31
YES
S32
要求者は、チームのチームマスタもしくは、subAUである
NO
改竄もしくは、不正行為があったとして、処理の中止
YES
S33
サブチームのAUD,AULの署名は、要求者のものである
NO
改竄もしくは、不正行為があったとして、処理の中止
YES
正常な権限でサブチームが作成されたと判断して、サブチームのAULとAUDを保存する
S34

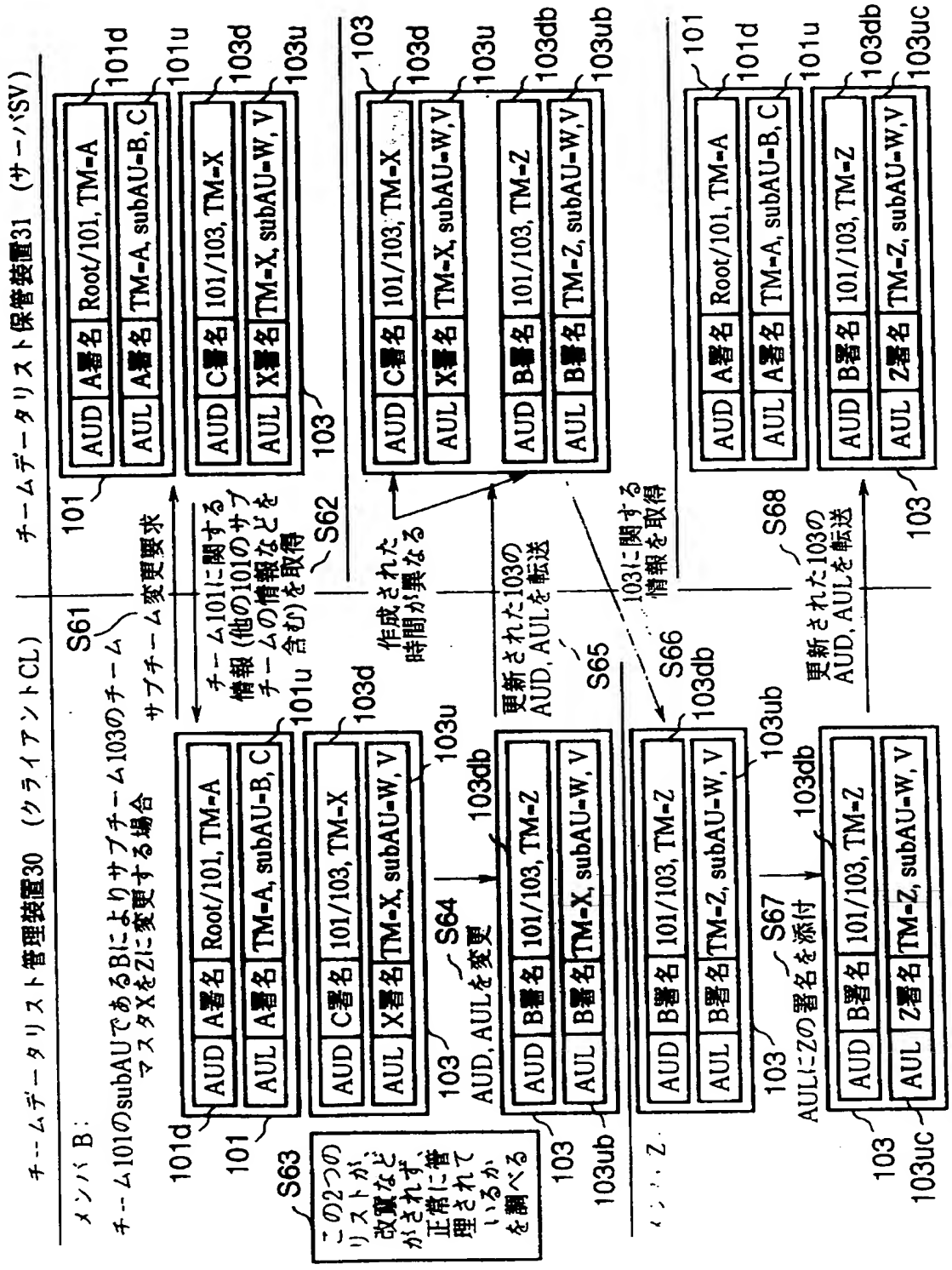
【図７】


リストの正当性の検証要求
S41
チームの
AUD, AULの署名確認、
改竄されていない
？
NO
不正行為が
あったとして
処理中止
YES
チームマスタの確認
S42
親チームの確認
S43
S44
親チームの
AUD, AULの署名確認
NO
不正行為が
あったとして
処理中止
YES
S45
チーム作成者は、
親チームのTMもしくは、
subAUである
？
NO
不正行為が
あったとして
処理中止
YES
S46
親チームがRootチーム
である?
NO
YES
Rootのチームマスタが確認できる
S47
ユーザによる承認
S48
S49
チーム階層を一つ上
の親チームに上がる

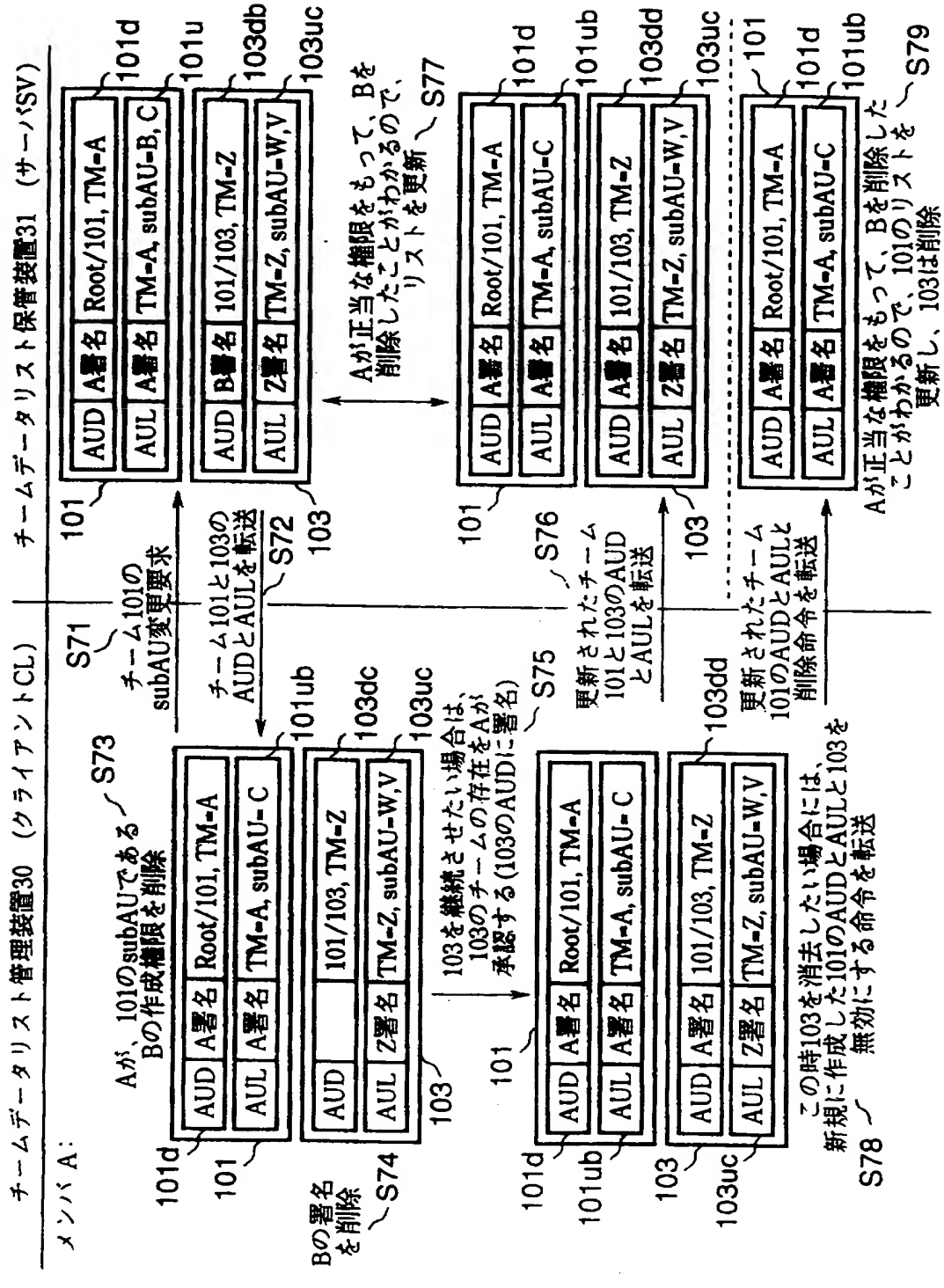
【図８】


要求者の識別
S51
YES
S52
要求者は、TMか、親チームのTM、もしくは subAUである
NO
正当な権限がないとして、処理の中止
YES
S53
AUDの署名者は、親チームのTM、もしくは、subAUである
NO
改竄もしくは、不正行為があったとして、処理の中止
YES
S54
AULの署名は、AUDに示されたTMの署名である
NO
改竄もしくは、不正行為があったとして、処理の中止
YES
正常な権限でサブチームが作成されたと判断して、サブチームのAULとAUDを保存
S55

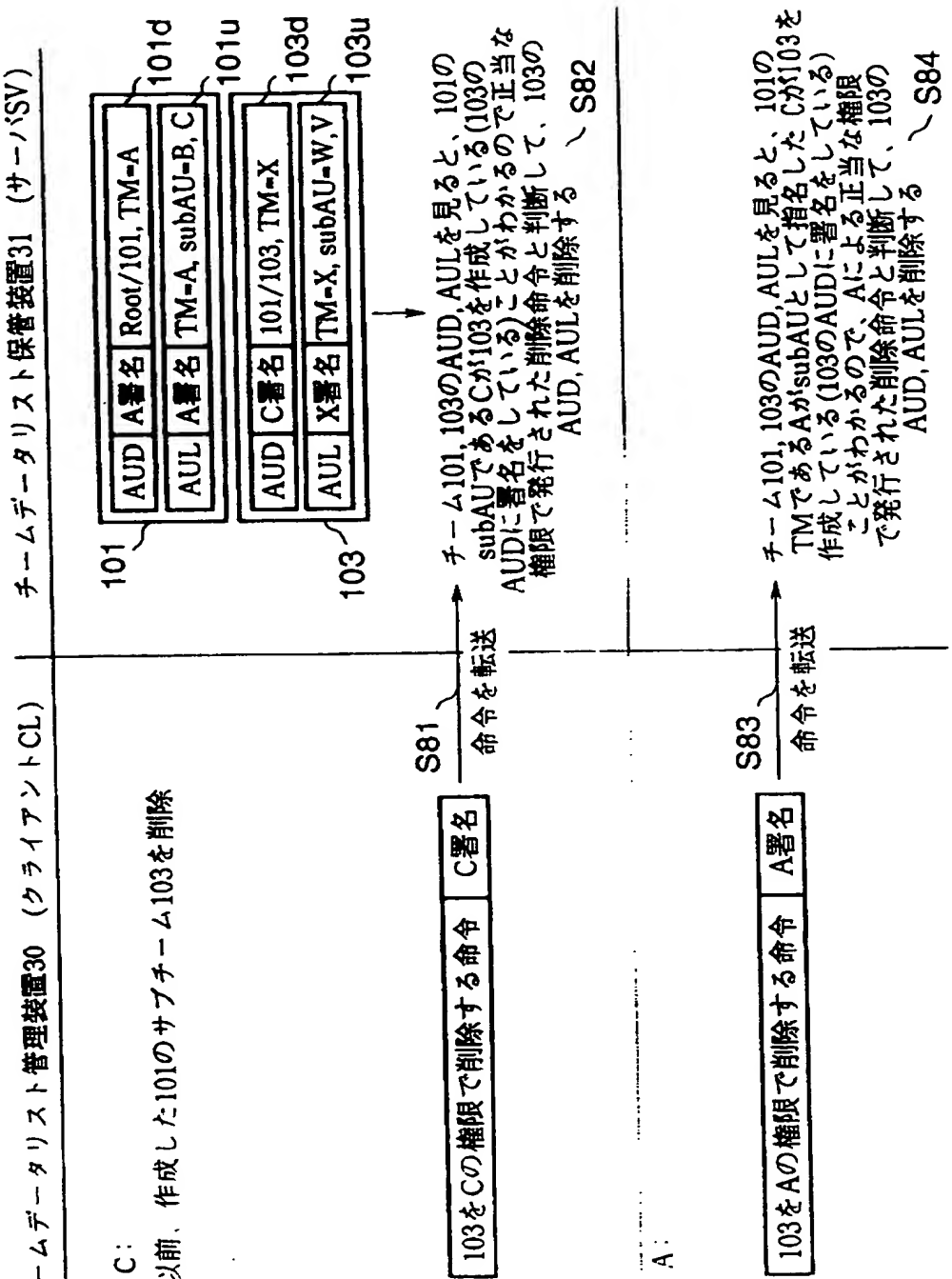
【図９】


チームデータリスト管理装置30 (クライアントCL)
チームデータリスト保管装置31 (サーバSV)
メンバB:
チーム101のsubAUであるBによりサブチーム103のチーム
マスタXをZに変更する場合
S61
サブチーム変更要求
101
AUD A署名 Root/101, TM-A
AUL A署名 TM-A, subAU-B, C
101d
101u
チーム101に関する
情報(他の101のサブ
チームの情報などを
含む)を取得
S62
AUD C署名 101/103, TM-X
AUL X署名 TM-X, subAU-W, V
103d
103u
103
作成された
時間が異なる
更新された103の
AUD, AULを転送
S65
103に関する
情報を取得
S66
S68
更新された103の
AUD, AULを転送
S63
このリストが、改竄などがされず、正常に管理されているかを調べる
AUD, AULを変更
S64
AUDにZの署名を添付
S67
103db
103ub
103uc
メンバ Z:

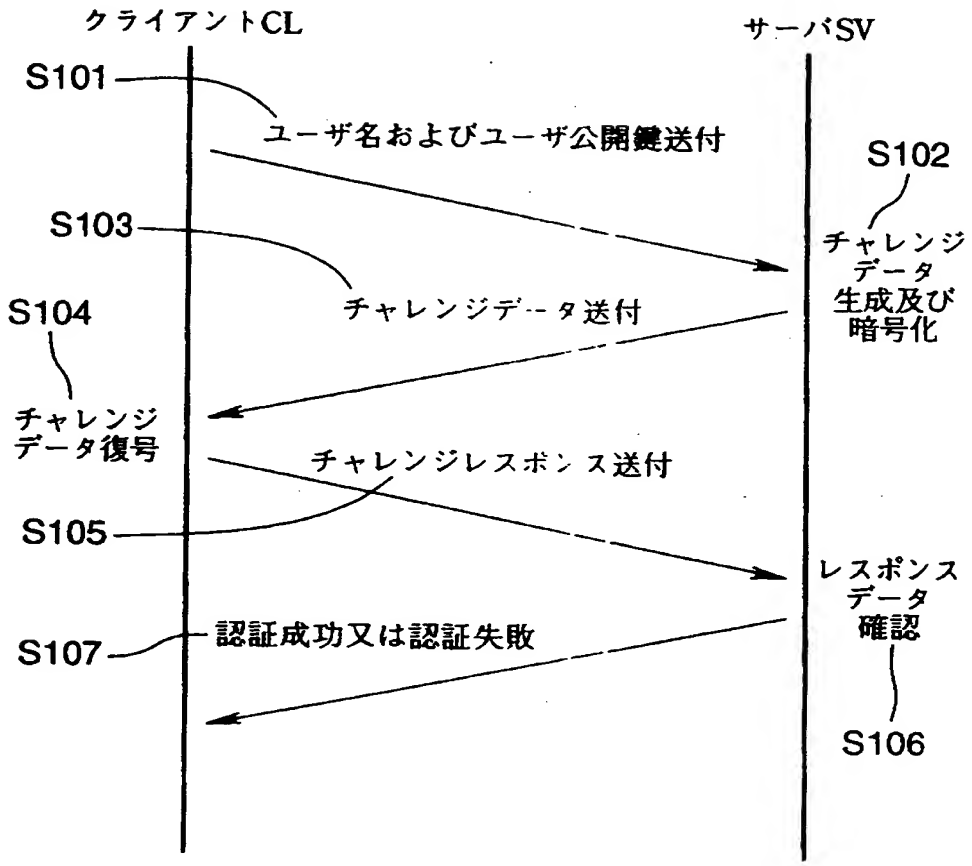
【図１０】


チームデータリスト管理装置30 （クライアントCL）
チームデータリスト保管装置31 （サーバSV）
メンバA:
S71
チーム101のsubAU変更要求
S72
チーム101と103のAUDとAULを転送
S73
Aが、101のsubAUである Bの作成権限を削除
S74
Bの署名を削除
S75
103を継続させたい場合は、103のチームの存在をAが承認する(103のAUDに署名)
S76
更新されたチーム101と103のAUDとAULを転送
S77
Aが正当な権限をもって、Bを削除したことがわかるので、リストを更新
S78
この時103を消去したい場合には、新規に作成した101のAUDとAULと103を無効にする命令を転送
更新されたチーム101のAUDとAULと削除命令を転送
S79
Aが正当な権限をもって、Bを削除したことがわかるので、101のリストを更新し、103は削除
AUD
AUL
A署名
B署名
Z署名
Root/101, TM-A
TM-A, subAU-B, C
101/103, TM-Z
TM-Z, subAU-W,V
TM-A, subAU-C
101d
101u
103db
103uc
101ub
103dc
103dd
101
103

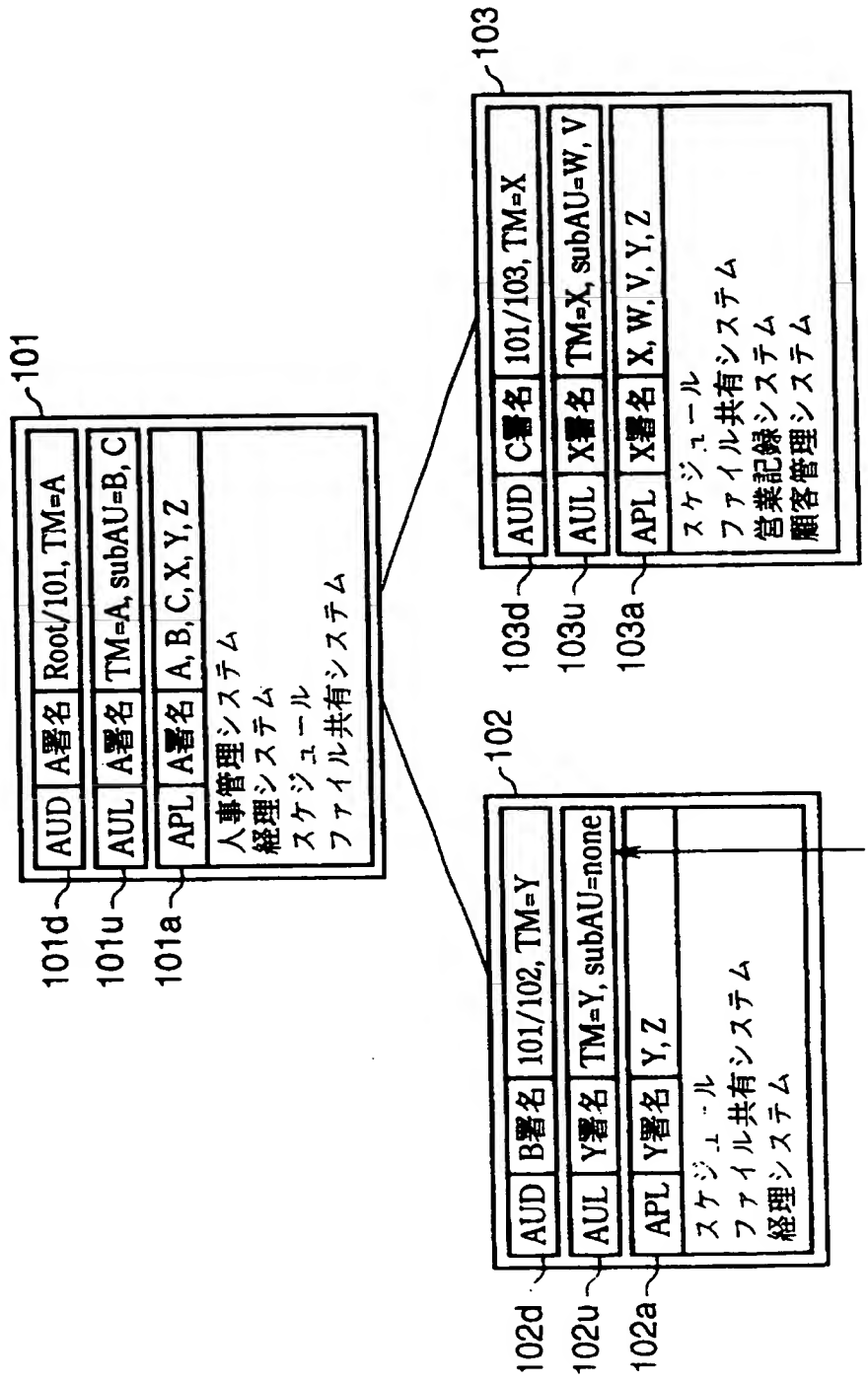
【図１１】


チームデータリスト管理装置30 (クライアントCL)
チームデータリスト保管装置31 (サーバSV)
メンバC:
以前、作成した101のサブチーム103を削除
101
AUD A署名 Root/101, TM-A
AUL A署名 TM-A, subAU-B, C
103
AUD C署名 101/103, TM-X
AUL X署名 TM-X, subAU-W, V
101d
101u
103d
103u
S81
103をCの権限で削除する命令 C署名
命令を転送
チーム101, 103のAUD, AULを見ると、101のsubAUであるCが103を作成している(103のAUDに署名をしている)ことがわかるので正当な権限で発行された削除命令と判断して、103のAUD, AULを削除する
S82
S83
103をAの権限で削除する命令 A署名
命令を転送
チーム101, 103のAUD, AULを見ると、101のTMであるAがsubAUとして指名したCが103を作成している(103のAUDに署名をしている)ことがわかるので、Aによる正当な権限で発行された削除命令と判断して、103のAUD, AULを削除する
S84

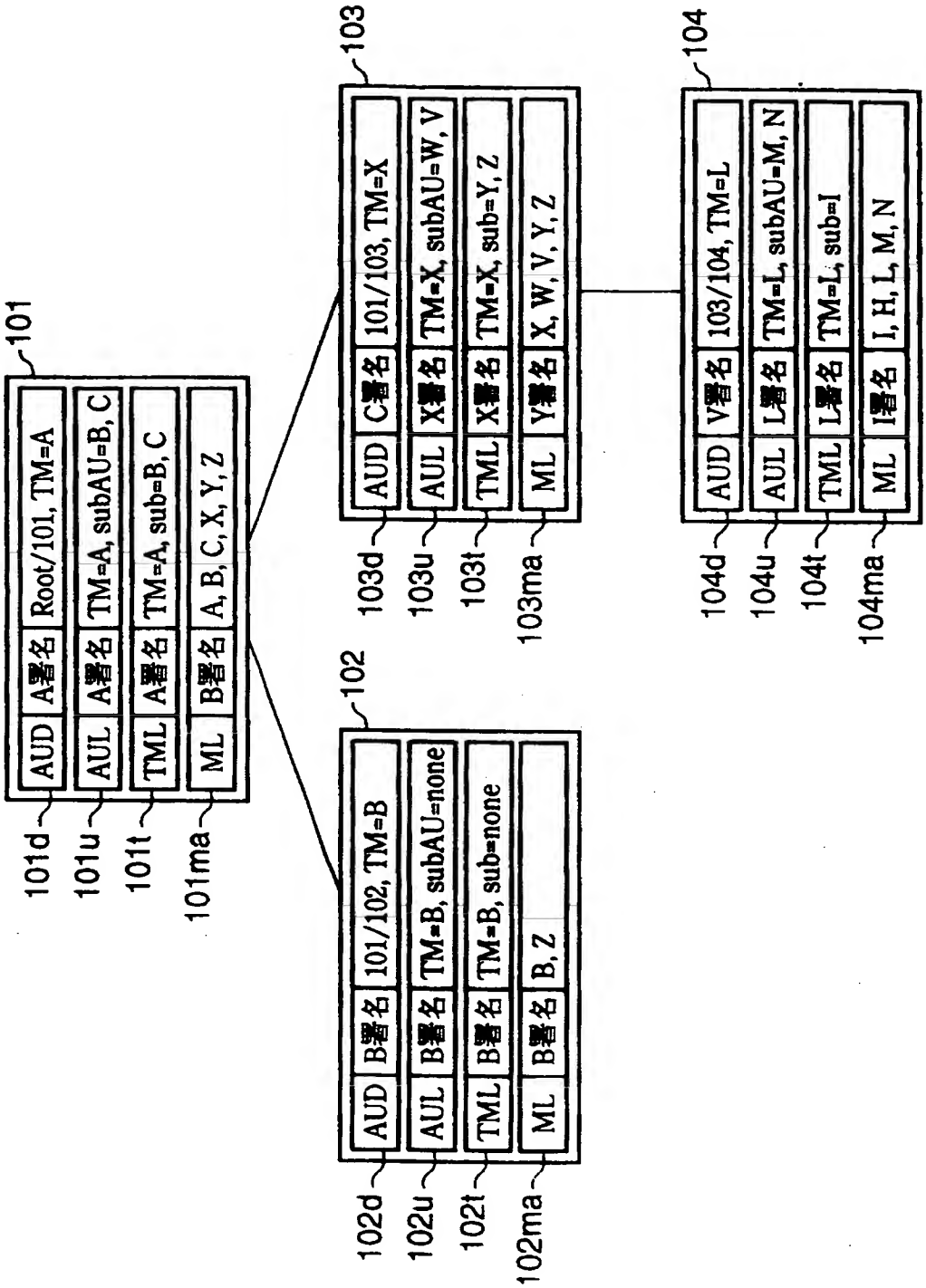
【図１２】


クライアントCL
サーバSV
S101
ユーザ名およびユーザ公開鍵送付
S102
チャレンジデータ生成及び暗号化
S103
チャレンジデータ送付
S104
チャレンジデータ復号
チャレンジレスポンス送付
S105
レスポンスデータ確認
S107
認証成功又は認証失敗
S106

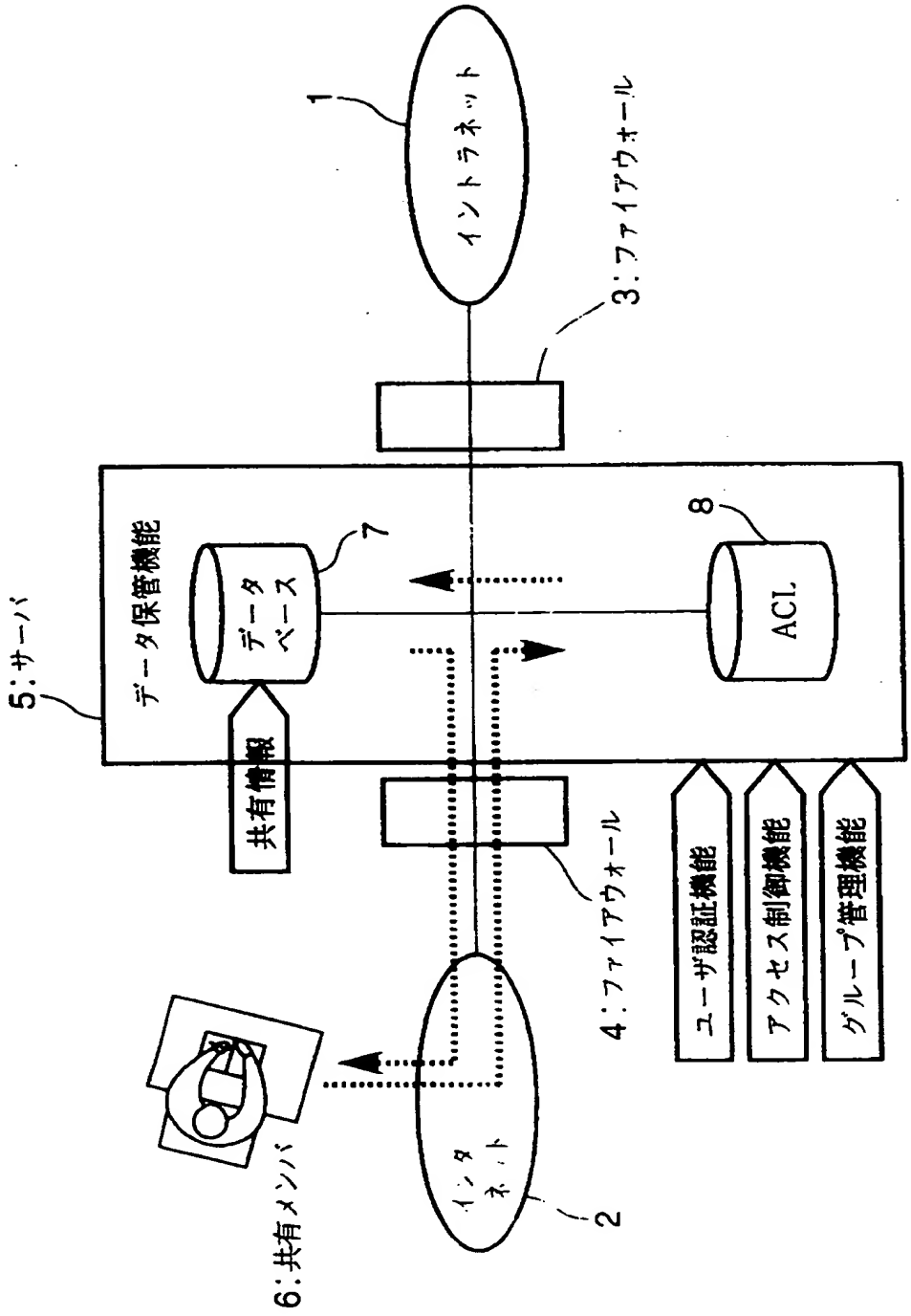
【図１３】


101
AUD
A署名
Root/101, TM=A
AUL
A署名
TM=A, subAU=B, C
APL
A署名
A, B, C, X, Y, Z
人事管理システム
経理システム
スケジュール
ファイル共有システム
101d
101u
101a
103
AUD
C署名
101/103, TM=X
AUL
X署名
TM=X, subAU=W, V
APL
X署名
X, W, V, Y, Z
スケジュール
ファイル共有システム
営業記録システム
顧客管理システム
103d
103u
103a
102
AUD
B署名
101/102, TM=Y
AUL
Y署名
TM=Y, subAU=none
APL
Y署名
Y, Z
スケジュール
ファイル共有システム
経理システム
102d
102u
102a

【図１４】


101
AUD
A署名
Root/101, TM=A
AUL
A署名
TM=A, subAU=B, C
TML
A署名
TM=A, sub=B, C
ML
B署名
A, B, C, X, Y, Z
101d
101u
101t
101ma
102
AUD
B署名
101/102, TM=B
AUL
B署名
TM=B, subAU=none
TML
B署名
TM=B, sub=none
ML
B署名
B, Z
102d
102u
102t
102ma
103
AUD
C署名
101/103, TM=X
AUL
X署名
TM=X, subAU=W, V
TML
X署名
TM=X, sub=Y, Z
ML
Y署名
X, W, V, Y, Z
103d
103u
103t
103ma
104
AUD
V署名
103/104, TM=L
AUL
L署名
TM=L, subAU=M, N
TML
L署名
TM=L, sub=I
ML
I署名
I, H, L, M, N
104d
104u
104t
104ma

【図１５】


1
イントラネット
3:ファイアウォール
5:サーバ
データ保管機能
データベース
7
8
ACL
共有情報
4:ファイアウォール
ユーザ認証機能
アクセス制御機能
グループ管理機能
6:共有メンバ
インターネット
2

【書類名】　要約書

【要約】

【課題】　複数のメンバで構成されるチームを階層化しつつ、情報や機能を共有できるチームデータリスト処理システムを提供する。

【解決手段】　オーソリティデータ３３はチームとその配下のサブチームの関係を表すデータ，オーソリティリスト３４は各チーム内の管理者を登録したリストであり、これらチームデータリストでチームの階層を規定する。リスト保管機能３６は記憶装置３２との間でチームデータリストを授受する。権限確認機能３５はチームデータリストの参照，変更，削除要求時にチームデータリストの内容を基に要求の許可，拒否を判断する。リスト正当性確認機能３７はチームデータリストの階層をルートチームに至るまで辿ってそのチームマスタの署名を確認する。ＡＵＤ・ＡＵＬ変更機能３８はチームデータリストの作成，削除，変更を行う。電子署名機能３９は公開鍵に対応する秘密鍵を取得し、変更されたチームデータリストに署名を付加する。

【選択図】　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000006264
【住所又は居所】　東京都千代田区大手町１丁目５番１号
【氏名又は名称】　三菱マテリアル株式会社
【代理人】　申請人
【識別番号】　100064908
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　志賀　正武
【選任した代理人】
【識別番号】　100108578
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　高橋　詔男
【選任した代理人】
【識別番号】　100089037
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　渡邊　隆
【選任した代理人】
【識別番号】　100101465
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　青山　正和
【選任した代理人】
【識別番号】　100094400
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　鈴木　三義
【選任した代理人】
【識別番号】　100106493
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　松冨　豊
【選任した代理人】

【識別番号】　100107836
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　西　和哉
【選任した代理人】
【識別番号】　100108394
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　今村　健一
【選任した代理人】
【識別番号】　100108453
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　村山　靖彦
【選任した代理人】
【識別番号】　100100077
【住所又は居所】　東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
【氏名又は名称】　大場　充

出　願　人　履　歴　情　報

識別番号　　〔０００００６２６４〕

１．変更年月日　　１９９２年　４月１０日
［変更理由］　住所変更
住　所　　東京都千代田区大手町１丁目５番１号
氏　名　　三菱マテリアル株式会社